.

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

Order Form

Call-Off Reference: P11590

Call-Off Title: Infected Blood Compensation Authority (IBCA) Data Delivery Partner

Call-Off Contract Description: The Infected Blood Compensation Authority (IBCA) require a Data Delivery Partner to support the ongoing development of the Data Platform

The Buyer: Infected Blood Compensation Authority

Buyer Address: 70 Whitehall, SW1A 2AS

The Supplier: Scott Logic Ltd

Supplier Address: 6th Floor, The Lumen, St James' Boulevard

Registration Number: 05377430

DUNS Number: 34-569-2490

SID4GOV ID: [**Insert** if known]

Applicable Framework Contract

This Order Form is for the provision of the Call-Off Deliverables and dated 16/12/2025.

It's issued under the Framework Contract with the reference number RM1043.8 for the provision of Digital Outcomes 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. **Call-Off Lot**

Lot 1- Digital Outcomes

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 Statements of Work

3 Joint Schedule 1 (Definitions) RM1043.8

4 Framework Special Terms

5 The following Schedules in equal order of precedence:

- Joint Schedules for RM1043.8 o Joint Schedule 2 (Variation Form) o Joint Schedule 3 (Insurance Requirements) o Joint Schedule 4 (Commercially Sensitive Information) o Joint Schedule 6 (Key Subcontractors) o Joint Schedule 7 (Financial Difficulties) o Joint Schedule 8 (Guarantee) **[NOT IN USED]** o Joint Schedule 10 (Rectification Plan) o Joint Schedule 11 (Processing Data) RM1043.8 o Joint Schedule 12 (Supply Chain Visibility) **[NOT IN USED]**
- Call-Off Schedules for RM1043.8 o Call-Off Schedule 1 (Transparency Reports) o Call-Off Schedule 2 (Staff Transfer) **[NOT IN USED]** o Call-Off Schedule 3 (Continuous Improvement) o Call-Off Schedule 5 (Pricing Details and Expenses Policy) o Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) o Call-Off Schedule 7 (Key Supplier Staff)
  - o Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - o Call-Off Schedule 9 (Security) o Call-Off Schedule 10 (Exit Management) o Call-Off Schedule 12 (Clustering) **[NOT IN USED]** o

Call-Off Schedule 13 (Implementation Plan and Testing) o CallOff Schedule 14 (Service Levels and Balanced Scorecard) o Call-Off Schedule 15 (Call-Off Contract Management) o Call-Off Schedule 16 (Benchmarking) **[NOT IN USED]** o Call-Off Schedule 17 (MOD Terms) **[NOT IN USED]** o Call-Off Schedule 18 (Background Checks) o Call-Off Schedule 19 (Scottish Law) **[NOT IN USED]** o Call-Off Schedule 20 (Call-Off Specification)

[Milestone Section 7 shall be NOT APPLICABLE]

o Call-Off Schedule 21 (Northern Ireland Law) **[NOT IN USED]** o Call-Off Schedule 23 (HMRC Terms) **[NOT IN USED]** o Call-Off Schedule 25 (Ethical Walls Agreement) **[NOT IN USED]** o Call-Off Schedule 26 (Cyber Essentials Scheme)

6 CCS Core Terms (version 3.0.11)

7 Joint Schedule 5 (Corporate Social Responsibility) RM1043.8

8 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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

Call-Off Special Terms

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

Special Term 1 : During the Term of this Agreement and for six (6) months thereafter, Buyer shall not, without the prior written consent of Supplier, directly solicit for employment any employee of Supplier who was actively involved in the performance of the Services. This restriction shall not apply to: (i) solicitations made through general public advertisements or job postings not specifically targeted at Supplier's personnel; or (ii) the hiring of any employee who is engaged by the Buyer without direct encouragement from Buyer.

Call-Off Start Date: **16/12/2025**

Call-Off Expiry Date: **15/12/2026**

Call-Off Initial Period: **1 Year**

Call-Off Optional Extension Period: **2 X 6 Month periods**

Minimum Notice Period for Extensions: **2 months**

Call-Off Contract Value: **TCV £7,500,000 excl. VAT (Y1 £5,000,000 excl.VAT; Y2 £2,500,000 excl. VAT)**

Call-Off Deliverables

Option B: See details in Call-Off Schedule 20 (Call-Off Specification)

Warranty Period

Unless specified in a Statement of Work, the Supplier shall provide the IP and warranties detailed in Paragraphs 4 (licensed Software warranty) and 9.6.2 (Specially Written Software and New IPRs) of Call-Off Schedule 6 (IPRs and Additional Terms on Digital Deliverables).

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). The Buyer requires the Supplier to comply with the following additional Standards for this Call-Off Contract:

ISO 27001

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.

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 £5,000,000

.

Call-Off Charges

1 Capped Time and Materials (CTM)

2 Incremental Fixed Price

3 Time and Materials (T&M)

4 Fixed Price

5 A combination of two or more of the above Charging methods.

Reimbursable Expenses

None unless specified in each Statement of Work

Payment Method

The payment terms and pricing model for each Statement of Work shall be set out in each Statement of Work.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs and sent to IBCA Deputy Director of Data Operations or their nominated delegate.

Invoices should be submitted to: ibcadeliv-finance@cabinetoffice.gov.uk and apinvoicescabu@gov.sscl.com

Any invoices must contain a valid PO number and the related supporting documentation

The Buyer may issue Supplier with a new PO number during the contract term, as it novates to an ALB.

Buyer's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

Buyer's Environmental Policy

Available online at: https://www.gov.uk/government/publications/cabientofficeenvironmental-policy-statement/cabinet-office-environmental-policy-statement

Buyer's Security Policy

As detailed in Attachment A

Supplier's Authorised Representative

REDACTED TEXT under FOIA Section 40, Personal Information

.

Supplier's Contract Manager

REDACTED TEXT under FOIA Section 40, Personal Information

Progress Report Frequency

On the first Working Day of each calendar month

Progress Meeting Frequency

Monthly on the first Working Week of each quarter

Key Staff

REDACTED TEXT under FOIA Section 40, Personal Information

Key Subcontractor(s)

REDACTED TEXT under FOIA Section 40, Personal Information

For the avoidance of doubt, the Supplier shall only be required to comply with the provisions relating to "subcontractors" under this Agreement with respect to the Key Subcontractors.

Commercially Sensitive Information

Supplier's Commercially Sensitive Information detailed in Schedule 4 and Schedule 20

Balanced Scorecard

See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)

Material KPIs

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

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Depencies KPI 1 - The Supplier's ability to fulfill the SOW and meet KPI 1 is contingent upon the Buyer providing access to all necessary information, systems, etc.
The Supplier shall notify the Buyer in writing of any lack of access to qualify for relief from associated service credits.

Service Credits

Service Credits will accrue in accordance with Call-Off Schedule 14 (Service Levels and Balanced Scorecard)

The Service Credit Cap is: 15% of total invoice value for the service period

The Service Period is: one Month, for the avoidance of doubt, where the KPI is assessed on quarterly basis, the service period is the month prior to the date on which the quarterly assessment has taken place.

A Critical Service Level Failure is:

(a) the Supplier accruing in the aggregate 5.5 more Service Points (in terms of the number of points allocated) in respect of the KPIs as outlined in the order form/ schedule 14 Attachments and/or any more than 15 Service Points for any Statement of Work in the relevant measurement period

(b) the Supplier accruing Service Credits or Compensation for Unacceptable KPI Failure which meet or exceed the Service Credit Cap;

Additional Insurances Not applicable

Guarantee

Not applicable

Social Value Commitment

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

Statement of Works

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

Signed - via Docusign
Supplier < Supplier Sign Here>
REDACTED TEXT under FOIA Section 40, Personal Information
Buyer < Commercial Sign Here>
REDACTED TEXT under FOIA Section 40, Personal Information

Appendix 1

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)].

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: 16/12/2025

SOW Title: IBCA Data Platform Discovery/Mobilisation SOW

SOW Reference: SOW/001

Call-Off Contract Reference: P11590

Buyer: Infected Blood Compensation Authority

Supplier: Scott Logic Limited

SOW Start Date: 16/12/2025

SOW End Date: 02/02/2026

Duration of SOW: 25 working days

Key Personnel (Buyer):

REDACTED TEXT under FOIA Section 40, Personal Information

Key Personnel (Supplier):

REDACTED TEXT under FOIA Section 40, Personal Information

Subcontractors:

REDACTED TEXT under FOIA Section 40, Personal Information

2 **Call-Off Contract Specification – Deliverables Context SOW Deliverables Background**: **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

Delivery phase(s): Beta

Overview of Requirement: **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

3 **Buyer Requirements – SOW Deliverables Outcome Description:**

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Delivery Plan:

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Dependencies:

To complete this work we will require from the Authority:

1. Suitably knowledgeable person(s) to deliver or participate in each of the workshops identified in the Delivery Plan, within the outlined schedule
2. Access to the materials, data and people for each of the activities identified in the Delivery Plan
3. Time to talk through each of the deliverables identified in the Delivery Plan, with the authority to evaluate whether the Acceptance Criteria have been met **Supplier Resource Plan:**

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

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 A **Cyber Essentials Scheme:**

The Buyer requires the Supplier to have and maintain a **Cyber Essentials Plus Certificate** for the work undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

SOW Standards:

The Supplier shall comply with the relevant (and current as of the Call-Off Start Date) Standards referred to in Framework Schedule 1 (Specification).

Performance Management:

Material KPIs	Target	Measured by
The IBCA Data Platform programme delivery plan is reported on weekly.	100% of weekly delivery reports submitted on time	Receipt of weekly report
Delivery of milestones	100% of acceptance criteria signed-off by the Buyer	Written acceptance/sign-off confirming from the Buyer criteria have been accepted

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:

REDACTED TEXT under FOIA Section 40, Personal Information

SOW Reporting Requirements:

Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

Ref.	Type of Information	Which Services does this requirement apply to?	Required regularity of Submission
1	The IBCA Data Platform programme delivery plan is	Delivery of the milestones	Weekly
	reported on weekly.		

4 Charges

Call Off Contract Charges:

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

The ceiling value of this SOW (irrespective of the selected charging method) is **£440,650 (excl. VAT)**

Payment Terms:

Invoices will be raised on a monthly basis in arrears and shall be payable within 30 days of the date of each invoice.

Rate Cards Applicable:

The basis of this calculation is set out in the call-off schedule 5 (Pricing Details and Expenses Policy). All rates are excl. VAT.

Reimbursable Expenses:

Reimbursable Expenses are capped at £0 under this Statement of Work.

Working Location:

Work shall be conducted in a hybrid working manner, between IBCA offices in Newcastle, the Supplier's offices and the individuals' remote working environments. Individuals shall attend the IBCA offices a minimum of 2 days per month but shall not be required (unless otherwise agreed) to attend more than 2 days per calendar week.

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:

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: IBCA Data Platform SOW A

SOW Reference:

Call-Off Contract Reference: P11590

Buyer: Infected Blood Compensation Authority

Supplier:Scott Logic Limited

SOW Start Date:

SOW End Date:

Duration of SOW:

Key Personnel (Buyer):

Key Personnel (Supplier):

Subcontractors:

Call-Off Contract Specification – Deliverables Context

SOW Deliverables Background

1.

Delivery phase(s):

Overview of Requirement:

2 **Buyer Requirements – SOW Deliverables Outcome Description**

Milestone Description:

The Supplier shall meet the following milestones through the delivery of outcomes:

Milestone Ref	Milestone Description	Acceptance Criteria	Due Date
MS01			
MS02			

Delivery Plan:

Dependencies:

Supplier Resource Plan:

Security Applicable to SOW:

The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part A 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 here] Cyber Essentials Scheme:**

The Buyer requires the Supplier to have and maintain a **Cyber Essentials Plus Certificate** for the work undertaken under this SOW, in accordance with Call-Off Schedule 26 (Cyber Essentials Scheme).

SOW Standards:

[**Insert** any specific Standards applicable to this SOW] **Performance Management:**

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

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 Role	**Key Staff**	**Contract Details**	**Worker Engagement Route (incl. inside/outside IR35)**

Key Supplier Staff:

SOW Reporting Requirements:

Further to the Supplier providing the management information detailed in Call-Off Schedule 15 (Call Off Contract Management), the Supplier shall also provide the following additional management information under and applicable to this SOW only:

Ref.	Type of Information	Which Services does this requirement apply to?	Required regularity of Submission
1.	[**insert**]		
1.1	[insert]	[insert]	[insert]

3 **Charges**

Call Off Contract Charges:

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

1. [Capped Time and Materials]
2. [Incremental Fixed Price]
3. [Time and Materials]
4. [Fixed Price]
5. [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 CallOff 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: None

4 **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:

Annex 1 Data Processing

The contact details of the Infected Blood Compensation Authority's Data Protection Officer are:

REDACTED TEXT under FOIA Section 40, Personal Information

The contact details of the Supplier's Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**

Description	Details
Identity of Controller for each Category of Personal Data	**The Infected Blood Compensation Authority is Controller and the Supplier is Processor** **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

Duration of the Processing	For the duration of the services.
Nature and purposes of the Processing	The purpose is to deliver the services as set out in this Statement of Work. The nature of the processing means any operation such as 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 data (whether or not by automated means) etc.
Type of Personal Data	**REDACTED TEXT under FOIA Section 40, Personal Information**

Categories of Data Subject	**REDACTED TEXT under FOIA Section 40, Personal Information**
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All processing of personal data by the Supplier will be undertaken on IT provided by the Authority. No plan for return and destruction is required as a result of personal data processing being undertaken by the Supplier within Authority infrastructure.

Call-Off Schedule 1 (Transparency Reports)

1 Transparency Reports

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note0117update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule. **Annex A: List of Transparency Reports**

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance metrics	Performance against SLA outlined in Call-Off Schedule 14 or as agreed for each SOW	Word and excel	Monthly
Call-Off Contract Charges	Details of work undertaken and payments made	Word and excel	Monthly
Resource plan	Details of types of resource planned to be used on the SOW's	Word and excel	Monthly
Performance and underperformance management	Details of any underperformance and plan for rectification	Word	Monthly

Call-Off Schedule 3 (Continuous Improvement)

1 Buyer's Rights

1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2 Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supplychains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 4 (Call-Off Tender)

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Call-Off Schedule 5 (Pricing Details and Expenses Policy)

The following rates shall be applied for the following categories of staff by the Supplier.

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

1 Call-Off Contract Charges

1.1 The Supplier shall provide:

1.1.1 as part of the Further Competition Procedure, its pricing for the Deliverables is in accordance with the Buyer's Statement of Requirements.

1.1.2 for each individual Statement of Work (SOW), the applicable Charges shall be calculated in accordance with the Pricing Mechanisms detailed in the Order Form using all of the following:

(a) the agreed rates for Supplier Staff and/or facilities (which are exclusive of any applicable expenses and VAT) incorporated into the Call-Off Contract; and

(b) the number of Work Days, or pro rata portion of a Work Day (see Paragraph 2.3.1 of Framework Schedule 3 (Framework Pricing)), that Supplier Staff work solely to provide the Deliverables and/or the provision of facilities solely to be used for the Buyer's stated purposes of providing the Deliverables and to meet the tasks sets out in the SOW between the SOW Start Date and SOW End Date.

1.2 Further to Paragraph 2.2.2 of Framework Schedule 3 (Framework Pricing), the Supplier will provide a detailed breakdown of its Charges for the Deliverables in sufficient detail to enable the Buyer to verify the accuracy of any invoice submitted.

This detailed breakdown will be incorporated into each SOW and include (but will not be limited to):

- a role description of each member of the Supplier Staff;
- a facilities description (if applicable);
- the agreed day rate for each Supplier Staff;
- any expenses charged for each Work Day for each Supplier Staff, which must be in accordance with the Buyer's expenses policy (if applicable);
- the number of Work Days, or pro rata for every part day, they will be actively be engaged in providing the Deliverables between the SOW Start Date and SOW End Date; and ● the total SOW cost for all Supplier Staff role and facilities in providing the Deliverables.

1.3 If a Capped or Fixed Price has been agreed for a particular SOW:

- the Supplier shall continue to work on the Deliverables until they are satisfactorily complete and accepted by the Buyer at its own cost and expense where the Capped or Fixed Price is exceeded; and
- the Buyer will have no obligation or liability to pay any additional Charges or cost of any part of the Deliverables yet to be completed and/or Delivered after the Capped or Fixed Price is exceeded by the Supplier.

1.4 All risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges:

1.4.1 The Supplier shall not charge expenses for members of Supplier Staff attending the Buyer's offices located in the Newcastle area.

1.4.2 The Buyer shall be providing all IT infrastructure hardware and software at its own cost for the Supplier Staff to utilise in the delivery of the Services.

Annex 1 (Expenses Policy)

https://intranet.cabinetoffice.gov.uk/information-for-employees/travel-for-work/introduction-totravel-and-expenses/

Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) 1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Buyer Property	the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Contract;
Buyer Software	any software which is owned by or licensed to the Buyer and which is or will be used by the Supplier for the purposes of providing the Deliverables;
Buyer System	the Buyer's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Buyer or the Supplier in connection with this Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
Commercial off the shelf Software or COTS Software	Non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;

Defect	any of the following: (a) any error, damage or defect in the manufacturing of a Deliverable; or (b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or (c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Call Off Contract; or (d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Contract;
Emergency Maintenance	ad hoc and unplanned maintenance provided by the Supplier where either Party reasonably suspects that the ICT Environment or the Services, or any part of the ICT Environment or the Services, has or may have developed a fault;
ICT Environment	the Buyer System and the Supplier System;
Licensed Software	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Call Off Contract, including any COTS Software;
Maintenance Schedule	has the meaning given to it in Paragraph 8 of this Schedule;

Malicious Software	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
New Release	an item produced primarily to extend, alter or improve the Software and/or any Deliverable by providing additional functionality or performance enhancement (whether or not defects in the Software and/or Deliverable are also corrected) while still retaining the original designated purpose of that item;
Open Source Software	computer software that has its source code made available subject to an open-source licence under which the owner of the copyright and other IPR in such software provides the rights to use, study, change and distribute the software to any and all persons and for any and all purposes free of charge;

Operating Environment	means the Buyer System and any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which: (a) the Deliverables are (or are to be) provided; or (b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; or (c) where any part of the Supplier System is situated;
Permitted Maintenance	has the meaning given to it in Paragraph 8.2 of this Schedule;
Quality Plans	has the meaning given to it in Paragraph 6.1 of this Schedule;
Sites	has the meaning given to it in Joint Schedule 1 (Definitions), and for the purposes of this Call-Off Schedule shall also include any premises from, to or at which physical interface with the Buyer System takes place;

Software	Specially Written Software COTS Software and non-COTS Supplier and third party Software;
Software Supporting Materials	has the meaning given to it in Paragraph 9.1 of this Schedule;
Source Code	computer programs and/or data in eye-readable form and in such form that it can be compiled or interpreted into equivalent binary code together with all related design comments, flow charts, technical information and documentation necessary for the use, reproduction, maintenance, modification and enhancement of such software;
Specially Written Software	any software (including database software, linking instructions, test scripts, compilation instructions and test instructions) created by the Supplier (or by a Sub-Contractor or other third party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR; and
Supplier System	the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related
	cabling (but excluding the Buyer System).

2 When this Schedule should be used

2.1 This Schedule is designed to provide additional provisions on Intellectual Property Rights for the Digital Deliverables.

3 Buyer due diligence requirements

3.1 The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;

3.1.1 suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;

3.1.2 operating processes and procedures and the working methods of the Buyer;

3.1.3 ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and

3.1.4 existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.

3.2 The Supplier confirms that it has advised the Buyer in writing of:

3.2.1 each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;

3.2.2 the actions needed to remedy each such unsuitable aspect; and

3.2.3 a timetable for and the costs of those actions.

3.3 The Supplier undertakes:

3.3.1 and represents to the Buyer that Deliverables will meet the Buyer's acceptance criteria as set out in the Call-Off Contract and, if applicable, each Statement of Work; and

3.3.2 to maintain all interface and interoperability between third party software or services, and Specially Written Software required for the performance or supply of the Deliverables.

4 Licensed software warranty

4.1 The Supplier represents and warrants that:

4.1.1 it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;

4.1.2 all components of the Specially Written Software shall:

4.1.2.1 be free from material design and programming errors;

4.1.2.2 perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels and Balanced Scorecard) and Documentation; and

4.1.2.3 not infringe any IPR. 5 **Provision**

of ICT Services

5.1 The Supplier shall:

5.1.1 ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;

5.1.2 ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;

5.1.3 ensure that the Supplier System will be free of all encumbrances;

5.1.4 ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;

5.1.5 minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables.

6 Standards and Quality Requirements

6.1 The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it (**"Quality Plans"**).

6.2 The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them. Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

6.3 Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.

6.4 The Supplier shall ensure that the Supplier Personnel shall at all times during the Call-Off Contract Period:

6.4.1 be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;

6.4.2 apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and

6.4.3 obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7 ICT Audit

7.1 The Supplier shall allow any auditor access to the Supplier premises to:

7.1.1 inspect the ICT Environment and the wider service delivery environment (or any part of them);

7.1.2 review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;

7.1.3 review the Supplier's quality management systems including all relevant Quality Plans.

8 Maintenance of the ICT Environment

8.1 If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment (**"Maintenance Schedule"**) and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.

8.2 Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as **"Permitted Maintenance"**) in accordance with the Maintenance Schedule.

8.3 The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.

8.4 The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9 Intellectual Property Rights

9.1 Assignments granted by the Supplier: Specially Written Software

9.1.1 The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:

9.1.1.1 the Documentation, Source Code and the Object Code of the Specially Written Software; and

9.1.1.2 all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the **"Software Supporting Materials"**).

9.1.2 The Supplier shall:

9.1.2.1 inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;

9.1.2.2 deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

9.1.2.3 without prejudice to Paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royalty-free licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.

9.1.3 The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2 Licences for non-COTS IPR from the Supplier and third parties to the Buyer

9.2.1 Unless the Buyer gives its Approval the Supplier must not use any:

(a) of its own Existing IPR that is not COTS Software;

(b) third party software that is not COTS Software

9.2.2 Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grant to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables

(or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

9.2.3 Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

9.2.3.1 notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and

9.2.3.2 only use such third party IPR as referred to at Paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

9.2.4 Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

9.2.5 The Supplier may terminate a licence granted under Paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3 Licenses for COTS Software by the Supplier and third parties to the Buyer

9.3.1 The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.2 Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.3 Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

9.3.4 The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:

9.3.4.1 will no longer be maintained or supported by the developer; or

9.3.4.2 will no longer be made commercially available

9.4 Buyer's right to assign/novate licences

9.4.1 The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to Paragraph 9.2 (to:

9.4.1.1 a Central Government Body; or

9.4.1.2 to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.

9.4.2 If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in Paragraph 9.2.

9.5 Licence granted by the Buyer

9.5.1 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6 Open Source Publication

9.6.1 Unless the Buyer otherwise agrees in advance in writing (and subject to Paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:

9.6.1.1 suitable for publication by the Buyer as Open Source; and

9.6.1.2 based on Open Standards (where applicable), and the Buyer may, at its sole discretion, publish the same as Open Source.

9.6.2 The Supplier hereby warrants that the Specially Written Software and the New IPR unless otherwise directed by the Buyer:

9.6.2.1 are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;

9.6.2.2 have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;

9.6.2.3 do not contain any material which would bring the Buyer into disrepute;

9.6.2.4 can be published as Open Source without breaching the rights of any third party;

9.6.2.5 will be supplied in a format suitable for publication as Open Source (**"the Open Source Publication Material"**) no later than the date notified by the Buyer to the Supplier; and

9.6.2.6 do not contain any Malicious Software.

9.6.3 Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:

9.6.3.1 as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and

9.6.3.2 include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7 Malicious Software

9.7.1 The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

9.7.2 If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.

9.7.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 9.7.2 shall be borne by the Parties as follows:

9.7.3.1 by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

9.7.3.2 by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10 **IPR asset management**

10.1 The Parties shall work together to ensure that there is appropriate IPR asset management under each Call-Off Contract, and:

10.1.1 where the Supplier is working on the Buyer's System, the Supplier shall comply with the Buyer's IPR asset management approach and procedures.

10.1.2 where the Supplier is working on the Supplier's System, the Buyer will ensure that it maintains its IPR asset management procedures in accordance with Good Industry Practice.

Records and materials associated with IPR asset management shall form part of the Deliverables, including those relating to any Specially Written Software or New IPR.

10.2 The Supplier shall comply with any instructions given by the Buyer as to where it shall store all work in progress Deliverables and finished Deliverables (including all Documentation and Source Code) during the term of the Call-Off Contract and at the stated intervals or frequency specified by the Buyer and upon termination of the Contract or any Statement of Work.

10.3 The Supplier shall ensure that all items it uploads into any repository contain sufficient detail, code annotations and instructions so that a third-party developer (with the relevant technical abilities within the applicable role) would be able to understand how the item was created and how it works together with other items in the repository within a reasonable timeframe.

10.4 The Supplier shall maintain a register of all Open Source Software it has used in the provision of the Deliverables as part of its IPR asset management obligations under this Contract.

Call-Off Schedule 7 (Key Supplier Staff)

1 **Key Supplier Staff**

1.1 The Order Form lists the key roles (**"Key Roles"**) and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date and the Statement of Work lists the Key Roles and names of persons who the Supplier shall appoint to fill those Key Roles as of the SOW Start Date.

1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

1.4 The Supplier shall not remove or replace and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

1.4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

1.5 The Supplier shall:

1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

1.5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least one (1) Month's notice where an employee of the Supplier has resigned and 3 (three) Months' notice where the Supplier would like to rotate any employee;

1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables;

1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced;

1.5.6 on written request from the Buyer, provide a copy of the contract of employment or engagement (between the Supplier and Supplier Staff) for every member of the Supplier Staff made available to the Buyer under the Call-Off Contract when providing Deliverables under any Statement of Work;

1.5.7 on written request from the Buyer, provide details of start and end dates of engagement for all Key Staff filling Key Roles under any Statement of Work**[.[; and]**

1.5.8 [**Insert** any additional requirements].]

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery) 1

Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
BCDR Plan	has the meaning given to it in Paragraph 2.2 of this Schedule;
Business Continuity Plan	has the meaning given to it in Paragraph 2.3.2 of this Schedule;
Disaster	the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be unavailable);
Disaster Recovery Deliverables	the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
Disaster Recovery Plan	has the meaning given to it in Paragraph 2.3.3 of this Schedule;
Disaster Recovery System	the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;

Related Supplier	any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
Review Report	has the meaning given to it in Paragraph 6.3 of this Schedule; and
Supplier's Proposals	has the meaning given to it in Paragraph 6.3 of this Schedule.

2 BCDR Plan

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 At least ninety (90) Working Days after the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a **"BCDR Plan"**), which shall detail the processes and arrangements that the Supplier shall follow to:

2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and 2.2.2 the recovery of the Deliverables in the event of a Disaster

2.3 The BCDR Plan shall be divided into three sections:

2.3.1 Section1 which shall set out general principles applicable to the BCDR Plan;

2.3.2 Section 2 which shall relate to business continuity (the **"Business Continuity Plan"**); and

2.3.3 Section 3 which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3 General Principles of the BCDR Plan (Section 1)

3.1 Section 1 of the BCDR Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and

3.2.4 It details a process for the management of disaster recovery testing.

3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.

3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4 Business Continuity (Section 2)

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

4.2 The Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;

4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and

4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5 Disaster Recovery (Section 3)

5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:

5.2.1 loss of access to the Buyer Premises;

5.2.2 loss of utilities to the Buyer Premises;

5.2.3 loss of the Supplier's helpdesk or CAFM system;

5.2.4 loss of a Subcontractor;

5.2.5 emergency notification and escalation process;

5.2.6 contact lists;

5.2.7 staff training and awareness;

5.2.8 BCDR Plan testing;

5.2.9 post implementation review process;

5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;

5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.13 testing and management arrangements. 6 **Review**

and changing the BCDR Plan

6.1 The Supplier shall review the BCDR Plan:

6.1.1 on a regular basis and as a minimum once every six (6) Months;

6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.

6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a **"Review Report"**) setting out the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.

6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the

Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Deliverables.

7 Testing the BCDR Plan

7.1 The Supplier shall test the BCDR Plan:

7.1.1 regularly and in any event not less than once in every Contract Year;

7.1.2 in the event of any major reconfiguration of the Deliverables;

7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).

7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.

7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8 Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9 Circumstances beyond your control

The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Schedule 9 (Security) Development Security Schedule

1 Buyer Options

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

Buyer risk assessment (see Paragraph **Error! Reference source not found.**)		
The Buyer has assessed this Contract as:	a higher-risk agreement	☒
	a standard agreement	☐
Certifications (see Paragraph 10) (applicable only for standard risk agreements)		
Where the Buyer has assessed this Contract as a standard risk agreement, the Supplier must have the following Certifications (or equivalent):	Cyber Essentials Plus	☒
	Cyber Essentials	☐
	No certification required	☐
The Supplier must ensure that Higher-risk Sub-contractors have the following Certifications (or equivalent):	Cyber Essentials Plus	☒
	Cyber Essentials	☐
	No certification required	☐

The Supplier must ensure that Medium-risk Sub-contractors have the following Certifications (or equivalent):	Cyber Essentials Plus	☐
	Cyber Essentials	☒
	No certification required	☐
Buyer Security Policies (see Paragraph 6)		

The Buyer requires the Supplier to comply with the following policies relating to security management: • Information Security Summary Policy • IBCA Cyber and Information Security Governance Policy • Risk Management Policy • Data Classification Policy • Supplier & Third-Party Security Policy • Security Awareness & Training Policy • Acceptable Use Policy	☒
Secure by Design Questionnaire (Paragraph 12)	
The Buyer requires the Supplier to complete the Secure by Design Questionnaire	☒
Locations (see Paragraph 1 of the Security Requirements)	

	the United Kingdom only	☒

The Supplier and Sub-contractors may store, access or Handle Government Data in:	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☐
	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	☒
	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☐
	anywhere in the world not prohibited by the Buyer	☐
Locations for Development Activity (see Paragraph 1 of the Security Requirements)		☐
The Supplier and Subcontractors may undertake Development Activity in:	the United Kingdom only	☒

	any territory as permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State)	☐
	anywhere in the world not prohibited by the Buyer	☐

2 Supplier obligations

2.1 Where the Buyer has assessed this Contract as a higher-risk agreement, the Supplier must comply with all requirements of this Schedule 9 (Security).

2.2 Where the Buyer has assessed this Contract as a standard risk agreement, the Supplier must comply with all requirements of this this Schedule 9 (Security) except:

(a) Paragraph 11 (*Security Management Plan*);

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

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

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

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

(f) Paragraph 20 of the Security Requirements (*Access Control*).

2.3 Where the Buyer has not made an assessment in the table in Paragraph 0, the Parties must treat this Contract as a higher-risk agreement.

3 Definitions

3.1 In this Schedule 9 (Security):

"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;

"Backup and Recovery Plan" the document setting out the Suppliers' and Sub-contractors' plans for the back and recovery of any Government Data they Handle;

"Breach Action Plan" means a plan prepared under Paragraph 23.3 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 Contract, including the Government Data and the Code;

(b) 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 Contract, including the Government Data and the Code; and/or

(c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements;

(d) the installation of Malicious Software in the:

(i) Supplier Information Management System;

(ii) Development Environment; or

(iii) Developed System;

(e) 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

(f) 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 operated by or on behalf of Central Government Bodies; or
(ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment" means any hardware, computer or telecoms devices, and equipment that

"Certification Rectification Plan" means the requirements set out in Paragraph 10.3;

"Certification Requirements"

"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 19 of the Security Requirements;

CHECK Team Leader means an individual with a CHECK Scheme team leader qualification issued by the NCSC;

CHECK Team Member means an individual with a CHECK Scheme team member qualification issued by the NCSC;

"Certification Default" means the occurrence of one or more of the circumstances list Paragraph 10.4;

forms part of the Buyer System;

means the plan referred to in Paragraph 10.5(a);

"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;

	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 9 (Security); 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 is required to develop under this Contract;
"Development Activity"	means any activity relating to the development, deployment maintenance and upgrading of the Developed System, including: (a) coding; (b) testing; (c) code storage; and (d) 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 provided by the Supplier or a Subcontractor and 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;

"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12 to 16 and in the table below paragraph 16 of
"Code Review"	

https://www.gov.uk/government/publications/governmentsecurityclassifications/guidance-11-working-at-official-html;

"Government Data Register"	means the register of all Government Data the Supplier, or any Subcontractor, receives from or creates for the Buyer, produced and maintained in accordance with Paragraph 24 of the Security Requirements;
"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"**Handle**"	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;
"**Higher-risk Subcontractor**"	means a Sub-contractor that Handles Authority Data that the Authority, in its discretion, has designated as a Higher-risk Sub-contractor;
"**HMG Baseline Personnel Security Standard**"	means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baselinepersonnel-security-standard), as that document is updated from time to time;
ISO Certification	means either of the following certifications when issued by a UKASrecognised Certification Body: (a) ISO/IEC27001:2013, where the certification was obtained before November 2022, but only until November 2025; and (a) ISO/IEC27001:2022 in all other cases;
"**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 19.2 of the Security Requirements;
"**Medium-risk Subcontractor**"	means a Sub-contractor that Handles Authority Data that the Authority, in its discretion, has designated as a Higher-risk Sub-contractor;
"**Modules Register**"	means the register of Third-party Software Modules required for higher risk agreements by Paragraph 11.4 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/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-designprinciples/cybersecurity-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-quickreferenceguide/;
"**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/wwwprojecttop-ten/;
"**Privileged User**"	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
"**Prohibited Activity**"	means the storage, access or Handling of Government Data prohibited by a Prohibition Notice;
"**Prohibition Notice**"	means a notice issued under Paragraph 1.11 of the Security Requirements;
"**Protective Monitoring System**"	means the system implemented by the Supplier and its Sub-contractors under Paragraph 21.1 of the Security Requirements to monitor and analyse access to and use of the Supplier Information Management System, the Development Environment, the Government Data and the Code;
"Questionnaire Response"	means the Supplier's response to the Secure by Design Questionnaire;
"**Register of Support Locations and Third-party Tools**"	means document setting out, in respect of Support Locations and Thirdparty Tools:

(a) the nature of the activity performed at the Support Location or by the Third-party Tool on the Code or the Government 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 1 of the Security Requirements;

"**Relevant Certifications**" means:

(a) for the Supplier:

(i) in the case of a higher-risk agreement

(A) either:

(1) an ISO Certification in respect of the Supplier Information Management System; or

(2) where the Supplier Information Management System is included within the scope of a wider ISO Certification, that ISO Certification; and

(B) Cyber Essentials Plus;

(ii) in the case of a standard agreement, either:

(C) the certification selected by the Buyer in Paragraph 1; or

(D) where the Buyer has not selected a certification option, Cyber Essentials; and

(b) for Higher-risk Subcontractors and Medium-risk Sub- contractors, either:

(i) the certification selected by the Buyer in Paragraph 1; or

(ii) where the Buyer has not selected a certification option, Cyber Essentials, (or equivalent certifications);

"**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 19.14 to 19.18, addressing the vulnerabilities and findings in a IT Health Check report;

Remote Location means a location other than a Supplier's or a Sub-contractor's Site;

Remote Working means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;

Remote Working Policy the policy prepared and approved under Paragraph 3 of the Security Requirements under which Supplier Staff are permitted to undertake Remote Working;

Secure by Design Approach means the Secure by Design policy issued by the Cabinet Office as updated or replaced from time to time, currently found at: https://www.security.gov.uk/policy-and-guidance/secure-by- design/principles/;

Secure by Design Principles means the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time-to-time, currently found at https://www.security.gov.uk/guidance/secure-by-design/activities/tracking- secure-by-design-progress;

Secure by Design Questionnaire the questionnaire in 0 (*Secure by Design Questionnaire*), implementing the Secure by Design Principles issued by the Cabinet Office, as updated or replaced from time to time, currently found at https://www.security.gov.uk/policy-and-guidance/secure-by- design/activities/tracking-secure-by-design-progress/;

"**Secure Development** 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

Guidance"

(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 11 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;

"**Sub-contractor**" means, for the purposes of this Schedule 9 (Security) only, 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 Government Data,

and this definition shall apply to this Schedule 9 in place of the definition of Sub-Contractor in Schedule 1 *(Definitions).*

"**Sub-contractor Staff**" 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*);

"**Support Location**" means a place or facility where or from which individuals may access or Handle the Code or the Government Data;

"**Support Register**" means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Contracts in accordance with Paragraph 12 of the Security Requirements;

"**Third-party** means any module, library or framework that:

Software Module"	(d) is not produced by the Supplier or a Sub-contractor as part of the Development Activity; and (e) 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 Software used by the Supplier by which the Code or the Government Data is accessed, analysed or modified or some form of operation is performed on it;
"**UKAS**"	means the United Kingdom Accreditation Service;
"**UKAS-recognised Certification Body**"	means: (a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or (b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual recognition agreement recognising the technical equivalence of accredited conformity assessment.

4 Introduction

4.1 This Schedule 9 (Security) sets out:

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

(i) higher risk agreement; or (ii) standard agreement, in Paragraph 01;

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

(i) the Development Activity;

(ii) the Development Environment;

(iii) the Government Data;

(iv) the Services; and

(v) the Supplier Information Management System;

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

(d) the Buyer's access to the Supplier Staff and Supplier Information Management System, in Paragraph 8;

(e) the Certification Requirements, in Paragraph 10;

(f) the requirements for a Security Management Plan in the case of higher-risk agreements, in Paragraph 11; and

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

5 Principles of Security

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

(a) the Buyer System;

(b) the Supplier System;

(c) the Sites;

(d) the Services; and

(e) the Supplier's Information Management System.

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

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

(a) the security, confidentiality, integrity and availability of the Government Data when that Government Data is under the control of the Supplier or any of its Subcontractors;

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

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

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

6 Security Requirements

6.1 The Supplier shall:

(a) comply with the Security Requirements; and

(b) where the relevant option in Paragraph 0 is selected, comply with the Buyer Security Policies;

(c) ensure that all Sub-contractors comply with:

(i) the Security Requirements; and

(ii) where the relevant option in Paragraph 0 is selected, the Buyer Security Policies,

that apply to the activities that the Sub-contractor performs under its Sub-contract, unless:

(iii) Paragraph 6.2 applies; or

(iv) the table in Annex 3 limits the Security Requirements that apply to a Subcontractor; and

(d) where the Buyer has assessed this Contract as a higher-risk agreement, ensure at all times that its provision of the Services and its operation and management of the Supplier Information Management System complies with the Security Management Plan.

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

(a) use reasonable endeavours to ensure that the SMP Sub-contractor complies with all obligations this Schedule 9 (Security) imposes on Sub-contractors, including the Security Requirements;

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

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

7 Staff

7.1 The Supplier must ensure that it all times it maintains within the Supplier Staff sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 9 (Security).

7.2 The Supplier must appoint:

(a) a senior individual within its organisation with accountability for managing security risks and the Supplier's implementation of the requirements of this Schedule 9 (Security); and

(b) a senior individual within the team responsible for the delivery of the Services with responsibility for managing the security risks to the Supplier Information Management System.

7.3 The individuals appointed under Paragraph 7.2:

(a) must have sufficient experience, knowledge and authority to undertake their roles effectively; and

(b) are to be designated as Key Staff and treated for the purposes of this Contract as Key Staff, whether or not they are otherwise designated as such;

7.4 The Supplier must review, and if necessary replace, the individuals appointed under Paragraph 7.2 if required to do so by the Buyer.

8 Access to Supplier Staff and Supplier Information Management System

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

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

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

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

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

8.2 The Supplier must provide the access required by the Buyer in accordance with Paragraph 8.1:

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

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

9 Government Data Handled using Supplier Information Management System

9.1 The Supplier acknowledges that the Supplier Information Management System: (a) is intended only for the Handling of Government Data that is classified as OFFICIAL; and

(b) is not intended for the Handling of Government Data that is classified as SECRET or TOP SECRET,

in each case using the Government Security Classification Policy.

9.2 The Supplier must:

(a) not alter the classification of any Government Data; and

(b) if it becomes aware that any Government Data classified as SECRET or TOP SECRET is being Handled using the Supplier Information Management System:

(i) immediately inform the Buyer; and

(ii) follow any instructions from the Buyer concerning that Government Data.

9.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with: (a) the Expected Behaviours; and

(b) the Security Controls.

9.4 Where there is a conflict between the Expected Behaviours or the Security Controls and this Schedule 9 (Security) the provisions of this Schedule 9 (Security) shall apply to the extent of any conflict.

10 Certification Requirements

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

(a) it; and

(b) any Higher-risk Sub-contractor and any Medium-risk Sub-contractor, is

certified as compliant with the Relevant Certifications

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

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

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

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

(a) currently in effect;

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

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

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

(a) a Relevant Certification in respect of the Supplier Information Management System has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification in respect of the Supplier Information Management System has expired and has not been renewed;

(c) the Relevant Certifications, together, no longer apply to the full scope of the Supplier Information Management System; or

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

(each a "Certification Default").

10.5 Where the Supplier has notified the Buyer of a Certification Default under Paragraph 10.4:

(a) the Supplier must, within 10 Working Days of the date in which the Supplier provided notice under Paragraph 10.4 (or such other period as the Parties may agree) provide a draft plan (a "Certification Rectification Plan") to the Buyer setting out:

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

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

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

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

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

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

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

11 Security Management Plan

11.1 This Paragraph 11 applies only where the Buyer has assessed that this Contract is a higherrisk agreement.

Preparation of Security Management Plan

11.2 The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule 9 (Security) and the Contract in order to ensure the security of the Development Environment, the Developed System, the Government Data and the Supplier Information Management System.

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

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

(b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System. the Government Data, the Buyer, the Services and/or users of the Services; and (c) the following information, so far as is applicable, in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any);

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

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

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

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

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

(vi) the Government Data Handled by the Sub-contractor;

(vii) the Handling that the Sub-contractor will undertake in respect of the Government Data;

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

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

(e) the Modules Register;

(f) the Support Register;

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

(i) the Secure Development Guidance; and

(ii) the secure development policy required by the ISO/IEC 27001:2022 Relevant Certifications;

(h) details of the protective monitoring that the Supplier will undertake in accordance with Paragraph 21 of the Security Requirements, including:

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

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

Approval of Security Management Plan

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

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

(i) undertake the Development Activity; and/or

(ii) Handle Government Data; or

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

11.5 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.

11.6 The process set out in Paragraph 11.5 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

11.7 The rejection by the Buyer of a second revised Certification Rectification Plan is a material Default of this Contract.

Updating Security Management Plan

11.8 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

11.9 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of: (a) a significant change to the components or architecture of the Supplier Information Management System;

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

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

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service; (g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

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

11.10 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.

12 Secure by Design Questionnaire

12.1 This Paragraph 12 applies only when the Buyer has selected the relevant option in Paragraph 1.

12.2 The Supplier must complete, by the date and in the format specified by the Buyer, and keep updated the Secure by Design Questionnaire

12.3 The Supplier must provide any explanations or supporting documents required by the Buyer to verify the contents of the Questionnaire Response.

12.4 The Supplier must ensure that at all times it provides the Services and operates and manages the Supplier System in the manner set out in its Questionnaire Response.

12.5 Where, at any time, the Buyer reasonably considers the Supplier's Questionnaire Responses do not, or do not adequately demonstrate the Supplier's compliance with:

(a) this Schedule;

(b) the Secure by Design Approach;

(c) the Security Management Plan (where applicable); or

(d) any applicable Buyer Security Policies,

the Supplier must, at its own costs and expense and by the date specified by the Buyer: (e) update the Supplier System to remedy the areas of non-compliance identified by the Buyer;

(f) update the Questionnaire Responses to reflect the changes to the Supplier System; and

(g) re-submit the Questionnaire Responses to the Buyer.

12.6 Where the Supplier considers that there is an inconsistency between the explicit or implicit requirements of the Secure by Design Questionnaire and the requirements of this Schedule 9 (Security), the Supplier must:

(a) immediately inform the Buyer; and

(b) comply with any instructions from the Buyer to resolve the inconsistency.

12.7 Where the instructions from the Buyer have the effect of imposing additional or different requirements on the Supplier than the requirements of this Schedule 9 (Security):

(a) the Parties must agree an appropriate Contract Change to amend this Schedule; and

(b) until the agreement of that Contract Change, any inconsistency must be resolved by applying the documents in the following order of precedence:

(i) the requirements of this Schedule 9 (Security);

(ii) the Secure by Design Questionnaire; and (iii) the Buyer

Security Policies.

13 Withholding of Charges

13.1 The Buyer may withhold some or all of the Charges in accordance with the provisions of this Paragraph 13 where:

(a) the Supplier in in material Default of any of its obligations under this Schedule 9 (Security); or

(b) any of the following matters occurs (where the those matters arise from a Default by the Supplier of its obligations under this this Schedule 9 (Security)):

(i) a Notifiable Default; (ii) an

Intervention Cause; or

(iii) a Step-In Trigger Event.

13.2 The Buyer may withhold a amount of the Charges that it considers sufficient, in its sole discretion, to incentivise the Supplier to perform the obligations it has Defaulted upon.

13.3 Before withholding any Charges under Paragraph 13.1 the Buyer must

(a) provide written notice to the Supplier setting out:

(i) the Default in respect of which the Buyer has decided to withhold some or all of the Charges;

(ii) the amount of the Charges that the Buyer will withhold;

(iii) the steps the Supplier must take to remedy the Default;

(iv) the date by which the Supplier must remedy the Default;

(v) the invoice in respect of which the Buyer will withhold the Charges; and

(b) consider any representations that the Supplier may make concerning the Buyer's decision.

13.4 Where the Supplier does not remedy the Default by the date specified in the notice given under Paragraph 13.3(a), the Buyer may retain the withheld amount.

13.5 The Supplier acknowledges:

(a) the legitimate interest that the Buyer has in ensuring the security of the Supplier Information Management System and the Government Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule 9 (Security); and

(b) that any Charges that are retained by the Buyer are not out of all proportion to the Buyer's legitimate interest, even where:

(i) the Buyer has not suffered any Losses as a result of the Supplier's Default; or

(ii) the value of the Losses suffered by the Buyer as a result of the Supplier's Default is lower than the amount of the Charges retained.

13.6 The Supplier may raise a Dispute under the Dispute Resolution Procedure with any decision by the Buyer to:

(a) withhold any Charges under Paragraph 13.1; or (b)

retain any Charges under Paragraph 13.4.

13.7 Any Dispute raised by the Supplier does not prevent the Buyer withholding Charges in respect of:

(a) the decision subject to the Dispute; or

(b) any other matter to which this Paragraph 13 applies.

13.8 Where any Dispute raised by the Supplier is resolved wholly or partially in its favour, the Buyer must return such sums as are specified in any agreement or other document setting out the resolution of the Dispute.

13.9 The Buyer's right to withhold or retain any amount under this Paragraph 13 are in addition to any other rights that the Buyer may have under this Contract or in Law, including any right to claim damages for Losses it suffers arising from the Default.

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 Subcontractors, at all times:

(a) undertake the Development Activity;

(b) host the Development Environment; and

(c) store, access or Handle Government Data,

(the "**Relevant Activities**") only in the geographic areas permitted by the Buyer in Paragraph 0.

1.2 Where the Buyer has not selected an option concerning location in Paragraph 0, the Supplier may only undertake the Relevant Activities in or from:

(a) the United Kingdom; or

(b) a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

1.3 The Supplier must, and must ensure 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 9 (Security);

(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 1.11.

1.4 Where the Supplier cannot comply with one or more of the requirements of Paragraph 1.3:

(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 Handle Government 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 Handle Government Data at that location, or those locations, as the Buyer may specify.

Support Locations

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

1.6 Where the Buyer has not selected an option concerning location in Paragraph 0, the Supplier may only undertake the Relevant Activities in or from:

(a) the United Kingdom; or

(b) a territory permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

1.7 the Supplier must, and must ensure 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 equivalent to those relating to Sub-contractors in this Schedule 9 (Security);

(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 1.11.

Third-party Tools

1.8 Before using any Third-party Tool, the Supplier must, and must ensure that its Subcontractors:

(a) enter into a binding agreement with the provider of the Third-party Tool;

(b) the binding agreement includes obligations on the provider in relation to security management equivalent to those relating to Sub-contractors in this Schedule 9 (Security);

(c) take reasonable steps to assure itself that the provider complies with the binding agreement;

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

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

(i) the provider;

(ii) the arrangements with the provider; and

(iii) the provider's compliance with the binding agreement; and (iv) the due diligence undertaken by the Supplier or Sub-contractor; and

(f) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

1.9 The Supplier must use, and ensure that Subcontractors use, only those Third-party Tools included in the Register of Sites, Support Locations and Third-party Tools.

1.10 The Supplier must not, and must not allow Sub-contractors to, use: (c) a Third-party Tool other than for the activity specified for that Third-party Tool in the Register of Sites, Support Locations and Third-party Tools; or

(d) a new Third-party Tool, or replace an existing Third-party Tool, without the permission of the Buyer. *Prohibited Activities*

1.11 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not:

(a) undertake or permit to be undertaken some or all of the Relevant Activities or operate Support Locations (a "**Prohibited Activity**").

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

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

(iii) in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity; or (b) use any specified Third-party Tool,

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

1.12 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice:

(a) undertakes any Prohibited Activities;

(b) uses any Support Locations; (c) or employs any Third-party Tool, 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 Physical Security

2.1 The Supplier must ensure, and must ensure that Sub-contractors ensure, that:

(a) all Sites, locations at which Relevant Activities are performed, or Support Locations (**Secure Locations**) have the necessary physical protective security measures in place to prevent unauthorised access, damage and interference, whether malicious or otherwise, to Government Data;

(a) the operator of the Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location; and

(b) the physical security risk assessment and site security plan for each Secure Location:

(i) considers whether different areas of the Secure Location require different security measures based on the functions of each area;

(ii) adopts a layered approach to physical security; (iii) has sections dealing with the following matters:

(A) the permitter of the Secure Location;

(B) the building fabric;

(C) security guarding;

(D) visitor and people management;

(E) server and communications rooms;

(F) protection of sensitive data;

(G) closed circuit television;

(H) automated access and control systems;

(I) intruder detection; and

(J) security control rooms.

2.2 The Supplier must provide the Buyer with the physical security risk assessment and site security plan for any Secure Location within 20 Working Days of a request by the Buyer.

3 Vetting, Training and Staff Access

Vetting before performing or managing Services

3.1 The Supplier must not engage Supplier Staff, and must ensure that Sub-contractors do not engage Sub-contractor Staff 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 3.2; or

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

3.2 For the purposes of Paragraph 3.1, the security checks are:

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

(i) the individual's identity;

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

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

(iv) that the individual has no Relevant Convictions;

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

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

Exception for certain Sub-contractors

3.3 Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Staff, 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 Staff 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 Staff and the management of the Subcontractor.

Annual training

3.4 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Staff, 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; and (c)

the Secure by Design Principles.

Staff access

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

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

3.7 Where requested by the Buyer, the Supplier must remove, and must ensure that Subcontractors remove, an individual Supplier Staff's access to the Government Data, or part of that Government Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

Remote Working

3.8 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

(a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;

(b) where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

3.9 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

(a) prepare and have approved by the Buyer the Remote Working Policy in accordance with this Paragraph;

(b) undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

(c) ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Staff of the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

3.10 The Remote Working Policy must include or make provision for the following matters: (a) restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Staff from downloading any Government Data to any End-user Device other than an End User Device that:

(i) is provided by the Supplier or Sub-contractor (as appropriate); and

(ii) complies with the requirements set out in Paragraph 4 (*End-user Devices*); (c) ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

(d) giving effect to the Security Controls (so far as they are applicable);

(e) for each different category of Supplier Staff subject to the proposed Remote Working Policy:

(i) the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

(ii) any identified security risks arising from the proposed Handling in a Remote Location;

(iii) the mitigations, controls and security measures the Supplier or Subcontractor (as applicable) will implement to mitigate the identified risks;

(iv) the residual risk levels following the implementation of those mitigations, controls and measures;

(v) when the Supplier or Sub-contractor (as applicable) will implement the proposed mitigations, controls and measures; and

(vi) the business rules with which the Supplier Staff must comply; and

(f) how the Supplier or the Subcontractor (as applicable) will:

(i) communicate the Remote Working Policy and business rules to Supplier Staff; and

(ii) enforce the Remote Working Plan and business rules.

3.11 The Supplier may submit a proposed Remote Working Policy to the Buyer for consideration at any time.

3.12 The Buyer must, within 20 Working Days of the submission of a proposed Remote Working Plan, either:

(a) approve the proposed Remote Working Policy, in which case the Supplier must, and ensure that any applicable Sub-contractor, implements the approved Remote Working Plan in accordance with its terms;

(b) reject the proposed Remote Working Policy, in which case:

(i) the Buyer may set out any changes to the proposed Remote Working Policy the Buyer requires to make the plan capable of approval; and

(ii) the Supplier may:

(A) revise the proposed Remote Working Plan; and

(B) re-submit the proposed Remote Working Plan to the Buyer for approval under Paragraph 3.11.

4 End-user Devices

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

(a) the operating system and any applications that store, Handle or have access to Government 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 Government Data and Code must be encrypted using a encryption tool agreed to by the Buyer;

(d) the End-under 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 Government Data and Code to ensure the security of that Government Data and Code;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the Enduser Device, remove or make inaccessible all Government 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.

4.2 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 Contract.

4.3 Where there any conflict between the requirements of this Schedule 9 (Security) and the requirements of the NCSC Device Guidance, the requirements of this Schedule take precedence.

5 Secure Architecture

5.1 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 Handle bulk data, the NCSC's guidance on "Bulk Data Principles"; and

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

5.2 Where any of the documents referred to in Paragraph 5.1 provides for various options, the Supplier must document the option it has chosen to implement and its reasons for doing so.

5.3 Notwithstanding anything in the specification for the Developed System or this Contract, the Supplier must ensure that the Developed System encrypts Government Data:

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

(b) when the Government Data is transmitted.

5.4 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 20.2 to 20.5 of the Security Requirements.

6 Secure Software Development by Design

6.1 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; and

(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 cyberattack techniques, including attacks using those vulnerabilities identified at any time in the OWASP Top Ten.

6.2 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.

6.3 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 nonautomated 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) is logically separate from all other environments, including production systems, operated by the Supplier or Sub-contractor;

(iii) requires 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; and

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

6.4 The Supplier must, and must ensure that all Sub contractors engaged in Development Activity, incorporate into the Developed System any security requirements identified:

(a) during any user research concerning the Developed System; or

(b) identified in any business case, or similar document, provided by the Buyer to the Supplier to inform its Development Activity.

7 Code Repository and Deployment Pipeline

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

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

7.2 ensure user access to cope 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

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 Contract 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 after each Code Review, the Supplier must provide the Buyer will 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 Handle Government Data where the licence terms of that software purport to grant the licensor rights to Handle the Government 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 Contract is a higherrisk 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 For the purposes of Paragraph 11.2(b), the Supplier must perform due diligence that is proportionate to the significance of the Third-party Software Module within the Code.

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

11.5 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.

11.6 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 Contract is a higherrisk agreement

12.2 Before using any software as part of the Supplier Information Management System, the Supplier must:

(a) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that software; and

(b) where there are any recognised security vulnerabilities, either:

(i) remedy vulnerabilities; or

(ii) ensure that the design of the Supplier Information Management System mitigates those vulnerabilities.

12.3 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.

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

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

(a) any vulnerabilities identified with the software and the steps the Supplier has taken to remedy or mitigate those vulnerabilities;

(i) within ten Working days of becoming aware of any new vulnerability in any item of software;

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

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

12.6 The Supplier must:

(a) review and update the Support Register:

(i) within 10 Working days of becoming aware of any new vulnerability in any item of software;

(ii) 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;

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

(iv) at least once every 12 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.

12.7 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.

12.8 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.

12.9 The Supplier must ensure that where any software or hardware component of the Supplier Information Management System is no longer required to provide the Services or has reached the end of its life it is removed or disconnected from the Supplier Information Management System.

13 Encryption

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

13.2 Before Handling any Government Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Handle Government Data will use to comply with this Paragraph 13.

13.3 Where this Paragraph 13 requires Government 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 Contract, the Supplier must ensure that the Developed System encrypts Government Data:

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

(b) when the Government Data is transmitted.

13.5 Unless Paragraph 13.6 applies, the Supplier must ensure, and must ensure that all Subcontractors ensure, that Government 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 Government Data as required by Paragraph 13.5, the Supplier must:

(a) immediately inform the Buyer of the subset or subsets of Government 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 Government Data concerned, the reasons why that Government 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 Government Data.

13.8 Where the Buyer and Supplier reach agreement, the Supplier must document: (a) the subset or subsets of Government 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 Government Data.

13.9 Where the Buyer and Supplier do not reach agreement within 10 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Government Data, either party may refer the matter to the NCSC.

14 Backup and recovery of Government Data

Backups and recovery of Government Data

14.1 The Supplier must backup and recover the Government Data in accordance with the Backup and Recovery Plan to ensure the recovery point objective and recovery time objective in Paragraph 14.3(a).

14.2 Any backup system operated by the Supplier or Sub-contractor forms part of the Supplier System or that Sub-contractor's System to which this Schedule 9 (Security) and the Security Requirements apply.

Backup and Recovery Plan

14.3 Unless otherwise required by the Buyer, the Backup and Recovery Plan must provide for: (a) in the case of a full or partial failure of the Supplier System or a Sub-contractor's System:

(i) a recovery time objective of less than 1 business day; and

(ii) a recovery point objective of up to 24 hours, and

(b) a retention period of 30 days.

14.4 In doing so, the Backup and Recovery Plan must ensure that in respect of any backup system operated by the Supplier or a Sub-contractor:

(a) the backup location for Government Data is sufficiently physically and logically separate from the rest of the Supplier System or a Sub-contractor's System that it is not affected by any Disaster affecting the rest of the Supplier System or a Subcontractor's System;

(b) there is sufficient storage volume for the amount of Government Data to be backed up;

(c) all back-up media for Government Data is used in accordance with the manufacturer's usage recommendations;

(d) newer backups of Government Data do not overwrite existing backups made during the retention period specified in Paragraph 14.3(a)(ii);

(e) the backup system monitors backups of Government Data to:

(i) identifies any backup failure; and

(ii) confirm the integrity of the Government Data backed up;

(f) any backup failure is remedied promptly;

(g) the backup system monitors the recovery of Government Data to:

(i) identify any recovery failure;

(ii) confirm the integrity of Government Data recovered; and

(h) any recovery failure is promptly remedied.

15 Email

15.1 Notwithstanding anything in the specification for the Developed System or this Contract, 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/setupgovernment-email-services-securely; or

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

16 DNS

16.1 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.

17 Malicious Software

17.1 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.

17.2 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.

17.3 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 Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

17.4 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 is a material Default.

18 Vulnerabilities

18.1 Unless the Buyer otherwise agrees, the Supplier must ensure that it or any relevant Subcontractor 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".

18.2 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 18.1.

18.3 For the purposes of this Paragraph 18, 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.

19 Security testing

Responsibility for security testing

19.1 The Supplier is solely responsible for:

(a) the costs of conducting any security testing required by this Paragraph 19; and

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

Security tests by Supplier

19.2 The Supplier must: (a) during the testing of the Developed System and before the Developed System goes live;

(b) at least once during each quarter, 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 19.8 to 19.10; and

(e) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph and 19.11 to 19.20.

19.3 In addition to its obligations under Paragraph 19.2, the Supplier must undertake any tests required by:

(a) any Remediation Action Plan;

(b) the ISO27001 Certification Requirements;

(c) the Security Management Plan; and

(d) the Buyer, following a Breach of Security or a significant change, as assessed by the Buyer, to the components or architecture of the Supplier Information Management System,

(each a Supplier Security Test).

19.4 The Supplier must:

(a) design and implement the Supplier Security Tests so as to minimise the impact on the delivery of the Services; (b) agree the date, timing, content and conduct of such Supplier Security Tests in advance with the Buyer.

19.5 Where the Supplier fully complies with Paragraph 19.4, if a Supplier Security Test causes a Performance Failure in a particular Measurement Period, the Supplier shall be entitled to relief in respect of such Performance Failure for that Measurement Period.

19.6 The Buyer may send a representative to witness the conduct of the Supplier Security Tests.

19.7 The Supplier shall provide the Buyer with a full, unedited and unredacted copy of the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable, and in any case within ten Working Days, after completion of each Supplier Security Test

IT Health Checks

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

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

(b) ensure that the CHECK Service Provider uses a qualified CHECK Team Leader and CHECK Team Members to perform the IT Health Check;

(c) 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.

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

(e) include within the scope of the IT Health Check such tests as the Buyer requires; (f) agree with the Buyer the scope, aim and timing of the IT Health Check.

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

19.10 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

19.11 In addition to complying with Paragraphs 19.13 to 19.20., 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.

19.12 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 19.11.

Significant vulnerabilities

19.13 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 Supplier Security Test report

19.14 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**").

19.15 Where the Buyer has commissioned a root cause analysis under Paragraph 19.13, the Supplier shall ensure that the draft Remediation Action Plan addresses that analysis.

19.16 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.

19.17 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.

19.18 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 19.16 to 19.18 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 19.19 and 19.20.

Implementing an approved Remediation Action Plan

19.19 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.

19.20 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. *Significant vulnerabilities*

19.21 Where:

(a) a Security Test report identifies more than 10 vulnerabilities classified as either critical or high; or

(b) the Buyer rejected a revised draft Remediation Action Plan,

the Buyer may, at the Supplier's cost, either:

(c) appoint an independent and appropriately qualified and experienced security architect and adviser to perform a root cause analysis of the identified vulnerabilities; or

(d) give notice to the Supplier requiring the appointment as soon as reasonably practicable, and in any event within ten Working Days, of an Independent Security Adviser.

20 Access Control

20.1 This Paragraph applies where the Buyer has assessed that this Contract is a higher-risk agreement.

20.2 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 Government 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.

20.3 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.

20.4 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.

20.5 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.

20.6 The Supplier must ensure that the Developed System is developed and configured so as to provide for the matters set out in Paragraphs 20.2 to 20.5.

20.7 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.

21 Event logging and protective monitoring

Protective Monitoring System

21.1 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 Government 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**").

21.2 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 Government 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

21.3 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

21.4 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

21.5 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.

22 Audit rights

Right of audit

22.1 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 9 (Security) and the Data Protection Laws as they apply to Government Data;

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

review the integrity, confidentiality and security of the Government Data; and/or

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

22.2 Any audit undertaken under this Paragraph 22:

(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 Contract.

22.3 The Buyer may not undertake more than one audit under Paragraph 22.1 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 Contract or the Data Protection Laws as they apply to the Government Data;

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

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

22.5 The Buyer 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.

22.6 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

22.7 Where an audit finds that:

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

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

22.8 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 Contract in respect of the audit findings.

23 Breach of Security

Reporting Breach of Security

23.1 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

23.2 The Supplier must, upon becoming aware of a Breach of Security immediately take those steps identified in the Security Management Plan 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

23.3 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 Breach of Security,

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

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

(a) in respect of each issue identified in the root cause analysis:

(i) how the issue will be remedied;

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

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

(b) the assistance the Supplier will provide to the Buyer to resolve any impacts on the Buyer, the Government Data and the Code;

(c) the Supplier's communication and engagement activities in respect of the Breach of Security, including any communication or engagement with individuals affected by any Breach of Security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data;

(d) the infrastructure, services and systems (including any contact centre facilities) the Supplier will establish to undertake the remediation, communication and engagement activities.

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

23.6 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 23.5 and 23.6 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.

23.7 When implementing the Breach Action Plan, the Supplier must:

(a) establish infrastructure, services and systems referred to in the Breach Action Plan;

(b) communicate and engage with affected individuals in accordance with the Breach Action Plan;

(c) communicate and engage with the Buyer and stakeholders identified by the Buyer in accordance with the Breach Plan and as otherwise required by the Buyer; and

(d) engage and deploy such additional resources as may be required to perform its responsibilities under the Breach Plan and this Contract in respect of the Personal Data Breach without any impact on the provision of the Services;

(e) continue to implement the Breach Action Plan until the Buyer indicates that the Breach of Security and the impacts on the Buyer, the Government Data, the Code and the affected individuals have been resolved to the Buyer's satisfaction.

23.8 The obligation to provide and implement a Breach Action Plan under Paragraphs 23.3 to 23.7 continues notwithstanding the expiry or termination of this Contract.

Costs of preparing and implementing a Breach Action Plan

23.9 The Supplier is solely responsible for its costs in preparing and implementing a Breach Action Plan.

Reporting of Breach of Security to regulator

23.10 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.

23.11 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) ensure so far as practicable the report it sends to the relevant regulator is consistent with the report provided by the Buyer.

24 Return and Deletion of Government Data

24.1 The Supplier must create and maintain a register of: (a) all Government 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 Government Data is stored,

(the "**Government Data Register**").

24.2 The Supplier must:

(a) review and update the Government Data Register:

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

(ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Government 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 Government Data Register: (i) whenever it updates the Government Data Register; and

(ii) otherwise when the Buyer requests.

24.3 Subject to Paragraph 24.4, the Supplier must, and must ensure that all Subcontractors, securely erase any or all Government Data held by the Supplier or Subcontractor, 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.

24.4 Paragraph 24.4 does not apply to Government Data:

(a) that is Personal Data in respect of which the Supplier is a Controller; (b) to which the Supplier has rights to Handle independently from this Contract; or

(c) in respect of which, the Supplier is under an obligation imposed by Law to retain.

24.5 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Government 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.

Annex 2 Security Management Plan Template

https://www.security.gov.uk/wp-content/uploads/2024/09/Appendix-XSecurityManagement-Plan-Template-Sept-24.docx

Annex 3 Sub-contractor Security Requirements

The table below sets out the Security Requirements that do **not** apply to particular categories of Sub-contractors.

	Higher-risk Sub-contractors	Medium-risk Sub-contractors	Sub-contractors
Security Requirements that do not apply			

Annex 4 Secure by Design Questionnaire

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
Principle 1 Create responsibility for cyber security risk Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities.	The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract.	
	The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery.	

	The Supplier provides adequate and appropriately qualified resources to support the Buyer with following the government Secure by Design Approach as part of service delivery. These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Buyer.	
Principle 2 Source secure technology products	The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the	

Secure by Design Principle	**Requirements**	**How the Supplier will meet the requirement**
Where third-party products are used, perform security due diligence by continually	significance associated with the product and are subject to agreement with the Buyer.	

assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.	The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Buyer's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Buyer should be informed and asked to accept the risk associated with using the product.	
	The Supplier takes reasonable steps to assess thirdparty products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Buyer. Where the product doesn't meet the required obligations, the Supplier must discuss with the Buyer the residual risks associated with using the product.	
Principle 3 Adopt a risk-driven approach	As provided by the Buyer, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	

Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections	The Supplier supports the Buyer with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
appropriate to the evolving threat landscape.	The Supplier supports the Buyer with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions. During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service.	
	The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach.	

	The Supplier factors in the legal and regulatory requirements provided by the Buyer in the risk management process and service design and build.	
Principle 4 Design usable security controls Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.	The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service.	
	The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls.	

Secure by Design Principle	**Requirements**	**How the Supplier will meet the requirement**

Principle 5 Build in detect and respond security Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate	The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the service.	
security logging, monitoring, alerting and response capabilities. These must be continually tested and iterated.	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation.	
	The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems.	

Principle 6 Design flexible architectures Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business requirements, cyber threats and vulnerabilities.	As agreed with the Buyer, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats and vulnerabilities.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	

Secure by Design Principle	**Requirements**	**How the Supplier will meet the requirement**
Principle 7 Minimise the attack surface Use only the capabilities, software, data and hardware	The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Buyer.	

components necessary for a service to mitigate cyber security risks while achieving its intended use.	The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Buyer's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit.	
	The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle.	
Principle 8 Defend in depth Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.	The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service.	
	The Supplier responsible for building the digital service implements security measures to incorporate segmentation.	
	The Supplier responsible for building the digital service implements mechanisms to keep the impact of potential security incidents contained.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 9 Embed continuous assurance Implement continuous security assurance processes to create confidence in the effectiveness of security controls, both at the point of delivery and throughout the operational life of the service.	The Supplier responsible for building the digital service reassess controls during build to ensure they operate effectively and that no known vulnerabilities exist.	
	The Supplier responsible for building the digital service reassesses security controls against changes in the service or threat landscape during the build phase.	
	The Supplier responsible for building the digital service reports on how the delivery team follows the Secure by Design Approach and adheres to the Secure by Design principles by contributing to the maintenance of the Secure by Design Self Assessment Tracker.	

Principle 10 Make changes securely Embed security into the design, development and deployment	The Supplier responsible for building the digital service works with the Buyer to assess the security impact of changes before these are made to digital services and infrastructure.	
processes to ensure that the security impact of changes is considered alongside other factors.	The Supplier responsible for building the digital service records any residual unmitigated risks to the cyber security risk register and shares this with the accountable individuals and security function responsible for incorporating these into the organisation's risk registers.	

Call-Off Schedule 10 (Exit Management) 1

Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Exclusive Assets	Supplier Assets used exclusively by the Supplier in the provision of the Deliverables;
Exit Information	has the meaning given to it in Paragraph 3.1 of this Schedule;
Exit Manager	the person appointed by each Party to manage their respective obligations under this Schedule;
Exit Plan	the plan produced and updated by the Supplier during the Initial Period in accordance with Paragraph 4 of this Schedule;
Net Book Value	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
Non- Exclusive Assets	those Supplier Assets used by the Supplier in connection with the Deliverables but which are also used by the Supplier for other purposes;
Registers	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
Replacement Goods	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
Replacement Services	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;

Termination Assistance	the activities to be performed by the Supplier pursuant to the Exit Plan, and other assistance required by the Buyer pursuant to the Termination Assistance Notice;
Termination Assistance Notice	has the meaning given to it in Paragraph 5.1 of this Schedule;
Termination Assistance Period	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
Transferable Assets	Exclusive Assets which are capable of legal transfer to the Buyer;
Transferable Contracts	Sub- Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
Transferring Assets	has the meaning given to it in Paragraph 8.2.1 of this Schedule; and
Transferring Contracts	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

2 Supplier must always be prepared for Contract exit and SOW exit

2.1 The Supplier shall within 30 days from the Call-Off Contract Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.

2.2 During the Contract Period, the Supplier shall promptly:

2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and

2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables which will be stored in the Deliverables IPR asset management system which includes all Document and Source Code repositories.

("**Registers**").

2.3 The Supplier shall:

2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and

2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.

2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Call-Off Contract Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of each SOW and this Contract.

3 Assisting re-competition for Deliverables

3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence whether this is in relation to one or more SOWs or the Call-Off Contract. (the "**Exit Information**").

3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.

3.3 The Supplier shall provide complete updates of the Exit Information on an asrequested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).

3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4 Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer a Call-Off Contract and SOW Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

4.3 The Exit Plan shall set out, as a minimum:

4.3.1 a detailed description of both the transfer and cessation processes, including a timetable (this may require modification to take into account the need to facilitate individual SOW Exit Plan provisions which shall be updated and incorporated as part of the SOW;

4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;

4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;

4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;

4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;

4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;

4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;

4.3.8 proposals for the disposal of any redundant Deliverables and materials;

4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and

4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.

4.4 The Supplier shall:

4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:

(a) prior to each SOW and no less than every [**six (6) Months**] throughout the Contract Period; and

(b) no later than [**twenty (20) Working Days**] after a request from the Buyer for an up-to-date copy of the Exit Plan;

(c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than [**ten (10) Working Days**] after the date of the Termination Assistance Notice;

(d) as soon as reasonably possible following, and in any event no later than [**twenty (20) Working Days**] following, any material change to the Deliverables (including all changes under the Variation Procedure); and

4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.

4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.

4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5 Termination Assistance

5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "**Termination Assistance Notice**") at least four (4) Months prior to the Expiry Date or, as soon as reasonably practicable, in the case of the Call-Off Contract and each SOW (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

5.1.1 the nature of the Termination Assistance required; and

5.1.2 the start date and initial period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the End Date.

5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the initial period specified in the Termination Assistance Notice in one or more extensions, in each case provided that:

5.2.1 no such extension shall extend the Termination Assistance Period beyond the date twelve (12) Months after the End Date; and

5.2.2 the Buyer shall notify the Supplier of any such extension no later than twenty (20) Working Days prior to the date on which the Termination Assistance Period is otherwise due to expire.

5.3 The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.

5.4 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6 Termination Assistance Period

6.1 Throughout the Termination Assistance Period the Supplier shall:

6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;

6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;

6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;

6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels or KPIs, the provision of the Management Information or any other reports or to any other of the Supplier's obligations under this Contract;

6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;

6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the deinstallation or removal of Supplier Assets is required.

6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.

6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels or KPIs, the Parties shall vary the relevant KPIs, Service Levels and/or the applicable Service Credits accordingly.

7 Obligations when the contract is terminated

7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.

7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:

7.2.1 vacate any Buyer Premises;

7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:

(a) such information relating to the Deliverables as remains in the possession or control of the Supplier; and

(b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.

7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8 Assets, Sub-contracts and Software

8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:

8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or

8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.

8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:

8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("**Transferring Assets**");

8.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets, the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "**Transferring Contracts**"), in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.

8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.

8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:

8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the

Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which

8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.

8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.

8.7 The Buyer shall:

8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and

8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.

8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.

8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9 **No charges**

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule other than those incurred in the ordinary course of business in delivering the services until the end of the Term, unless otherwise agreed in writing by the parties.

10 **Dividing the bills**

10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:

10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A: Implementation 1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition

Delay	(a) a delay in the Achievement of a Milestone by its Milestone Date; or (b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
Deliverable Item	an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
Milestone Payment	a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone; and
Implementation Period	The implementation plan to be prepared by the Supplier in accordance with this Schedule with respect to the Social Value Commitment only.

2 Agreeing and following the Implementation Plan

2.1 A draft of the Implementation Plan is set out in the Annex to this Schedule. The Supplier shall provide a further draft Implementation Plan **60 (sixty) days** after the Call-Off Contract Start Date.

2.2 The draft Implementation Plan:

2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively for the Social Value Commitment.

2.2.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.

2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is achieved on or before its Milestone Date.

2.5 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

3 Reviewing and changing the Implementation Plan

3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.

3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.

3.3 Changes to any Milestones, Milestone Payments and Delay Payments shall only be made in accordance with the Variation Procedure.

3.4 Time in relation to compliance with the Implementation Plan shall be of the essence and failure of the Supplier to comply with the Implementation Plan shall be a material Default.

4 Security requirements before the Start Date

4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in the Statement of Work 's Implementation Plans.

4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.

4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.

4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.

4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.

4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5 What to do if there is a Delay

5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:

5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;

5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;

5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and

5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.

6 Compensation for a Delay

6.1 If Delay Payments have been included in the Implementation Plan and a Milestone has not been achieved by the relevant Milestone Date, the Supplier shall pay to the Buyer such Delay Payments (calculated as set out by the Buyer in the Implementation Plan) and the following provisions shall apply:

6.1.1 the Supplier acknowledges and agrees that any Delay Payment is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to Achieve the corresponding Milestone;

6.1.2 Delay Payments shall be the Buyer's exclusive financial remedy for the Supplier's failure to Achieve a Milestone by its Milestone Date except where:

(a) the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4

(When CCS or the Buyer can end this contract); or

(b) the delay exceeds the number of days (the "**Delay Period Limit**") specified in the Implementation Plan commencing on the relevant Milestone Date;

6.1.3 the Delay Payments will accrue on a daily basis from the relevant Milestone Date until the date when the Milestone is Achieved;

6.1.4 no payment or other act or omission of the Buyer shall in any way affect the rights of the Buyer to recover the Delay Payments or be deemed to be a waiver of the right of the Buyer to recover any such damages; and

6.1.5 Delay Payments shall not be subject to or count towards any limitation on liability set out in Clause 11 (How much you can be held responsible for).

7 Implementation Plan

7.1 The Implementation Period will be for the entire duration of the Call-Off Contract and only for Social Value.

7.2 the Supplier shall:

7.2.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Plan, to ensure that the Implementation Plan is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.2.2 manage and report progress against the Implementation Plan;

7.2.3 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;

7.2.4 attend progress meetings in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and

7.2.5 ensure that all risks associated with the Implementation Period are minimised to ensure a seamless change of control between incumbent provider and the Supplier.

Annex 1: Implementation Plan

A.1 The Supplier shall provide a:

(a) high level Implementation Plan for the Social Value

A.2 The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

- Milestone: [ ]
- Deliverable Items: [ ]
- Duration: [ ]
- Milestone Date: [ ]
- Buyer Responsibilities: [ ]
- Milestone Payments: [ ]
- Delay Payments: [ ]

The Milestones will be Achieved in accordance with this Call-Off Schedule 13: (Implementation Plan and Testing)

For the purposes of Paragraph 6.1.2 the Delay Period Limit shall be [**insert number of days**].

Call-Off Schedule 14 (Service Levels and Balanced Scorecard)

SECTION 1: SERVICE LEVELS 1 Definitions

1.1 In this Section 1 of this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Critical Service	has the meaning given to it in the Order Form;
Level Failure	
Service Credits	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
Service Credit Cap	has the meaning given to it in the Order Form;
Service Level Failure	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
Service Level Performance Measure	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
Service Level Threshold	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

2 What happens if you do not meet the Service Levels

2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

2.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule, including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

2.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

2.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

2.4.3 the Buyer is entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

2.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

2.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

2.5.3 there is no change to the Service Credit Cap.

3 Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period **("Compensation for Critical Service Level Failure"**), provided that the operation of this Paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

Part A: Service Levels and Service Credits 1 Service Levels

If the level of performance of the Supplier:

1.1 is likely to or fails to meet any Service Level Performance Measure; or

1.2 is likely to cause or causes a Critical Service Failure to occur, the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

2 Service Credits

2.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

3 Buyer redress for failure to provide Services at or above Service Levels

3.1 The Buyer may ask for a Rectification Plan if the Supplier fails to meet [any][**OR**][Insert Number] of the Service Levels ("Default") within Section 1 (Service Levels) in any 12Month rolling period.

3.2 This Rectification Plan must clearly detail the improvements and associated timeframes within which the Supplier shall meet and achieve the Service Levels. The Rectification Plan must be provided in accordance with Clause 10.3 of the Core Terms and any failure to correct a Default in line with an accepted Rectification Plan, or failure to provide a Rectification Plan within 10 days of the request may result in the Buyer exercising its right to terminate the Contract in accordance with Clause 10.4 of the Core Terms.

Annex A to Part A: Services Levels and Service Credits Table

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Part B: Performance Monitoring 1 Performance Monitoring and Performance Review

1.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

1.2 The Supplier shall provide the Buyer with performance monitoring reports **("Performance Monitoring Reports"**) in accordance with the process and timescales agreed pursuant to Paragraph 1.1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

1.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

1.2.3 details of any Critical Service Level Failures;

1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

1.2.6 such other details as the Buyer may reasonably require from time to time.

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports **("Performance Review Meetings"**) on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location, format and time (within normal business hours) as the Buyer shall reasonably require;

1.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

1.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

1.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

1.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier for any specified Service Period.

2 Satisfaction Surveys

2.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Call-Off Schedule 15 (Call-Off Contract Management)

1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Operational Board	the board established in accordance with Paragraph 4.1 of this Schedule; and
Project Manager	the manager appointed in accordance with Paragraph 2.1 of this Schedule.

2 Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to Paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3 Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager's shall be:

3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4 Role of the Operational Board

4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5 Contract Risk Management

5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.

5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.2.1 the identification and management of risks; 5.2.2 the identification

and management of issues; and

5.2.3 monitoring and controlling project plans.

5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

5.4 The Supplier will maintain a risk register of the risks relating to the Call-Off Contract which the Buyer's and the Supplier have identified.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below: Monthly contract management meeting carried out at Infected Blood Compensation Authority, Benton Park View, Newcastle upon Tyne NE98 1XY United Kingdom

Call-Off Schedule 18 (Background Checks)

1 When you should use this Schedule

This Schedule should be used where Supplier Staff must be vetted before working on the Contract.

2 Definitions

Term	Definition

Relevant Conviction	means any conviction listed in Annex 1 to this Schedule.

3 **Relevant Convictions**

3.1 The Supplier must ensure that no person who discloses that they have a Relevant Conviction, or a person who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Deliverables without Approval.

3.2 Notwithstanding Paragraph 3.1 for each member of Supplier Staff who, in providing the Deliverables, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier must (and shall procure that the relevant Sub-Contractor must):

(a) carry out a check with the records held by the Department for Education (DfE);

(b) conduct thorough questioning regarding any Relevant Convictions; and

(c) ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS), and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Deliverables any person who has a Relevant Conviction or an inappropriate record.

Annex 1: Relevant Convictions

All staff must be SC cleared

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Call-Off Schedule 26 (Cyber Essentials Scheme)

1 **Definitions**

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	Definition
Cyber Essentials Scheme	the Cyber Essentials Scheme developed by the Government which provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats (as may be amended from time to time). Details of the Cyber Essentials Scheme are at: https://www.cyberessentials.ncsc.gov.uk/;

Cyber Essentials Basic Certificate	the certificate awarded on the basis of self-assessment, verified by an independent certification body, under the Cyber Essentials Scheme and is the basic level of assurance;
Cyber Essentials Certificate	Cyber Essentials Basic Certificate or the Cyber Essentials Plus Certificate to be provided by the Supplier as set out in the Order Form;
Cyber Essential Scheme Data	sensitive and personal information and other relevant information as referred to in the Cyber Essentials Scheme; and
Cyber Essentials Plus Certificate	the certification awarded on the basis of external testing by an independent certification body of the
	Supplier's cyber security approach under the Cyber Essentials Scheme and is a more advanced level of assurance.

2 What Certification do you need

2.1 Where the Order Form requires that the Supplier provide a Cyber Essentials Certificate or Cyber Essentials Plus Certificate prior to commencing the provision of Deliverables under the Call-Off Contract the Supplier shall provide a valid Cyber Essentials Certificate or Cyber Essentials Plus Certificate to the Buyer. Where the Supplier fails to comply with this Paragraph it shall be prohibited from commencing the provision of Deliverables under the Call-Off Contract until such time as the Supplier has evidenced to the Buyer its compliance with this Paragraph 2.1.

2.2 Where the Supplier continues to process data during the Call-Off Contract Period the Supplier shall deliver to the Buyer evidence of renewal of the Cyber Essentials Certificate or Cyber Essentials Plus Certificate on each anniversary of the first applicable certificate obtained by the Supplier under Paragraph 2.1.

2.3 In the event that the Supplier fails to comply with Paragraph 2.1 or 2.2, the Buyer reserves the right to terminate the Call-Off Contract for material Default.

2.4 The Supplier shall ensure that all Sub-Contracts with Subcontractors who Process Cyber Essentials Data contain provisions no less onerous on the Subcontractors than those imposed on the Supplier under the Call-Off Contract in respect of the Cyber Essentials Scheme under Paragraph 2.1 of this Schedule.

2.5 This Schedule shall survive termination of each and any Call-Off Contract.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the contract):

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer] ("**CCS**" / "**the Buyer**") And **[insert** name of Supplier] ("**the Supplier**")	
Contract name:	**[insert** name of contract to be changed] ("the Contract")	
Contract reference number:	**[insert** contract reference number]	
[Statement of Work (SOW) reference:]	**[insert** SOW reference number and title (if applicable) or delete row]	
[Buyer reference:]	**[insert** cost centre/portfolio codes as appropriate]	
Details of Proposed Variation		
Variation initiated by:	**[delete** as applicable: CCS/Buyer/Supplier]	
Variation number:	**[insert** variation number]	
Date variation is raised:	**[insert** date]	
Proposed variation	**[insert** detail here or use Annex 1 below]	
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: ● **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] ● **[reference Annex 1** as appropriate]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]

	New Contract value:	£ **[insert** amount]
[Timescale variation/s:]	**[insert** changes to dates/milestones or delete row]	

1 This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by [**delete** as applicable: CCS / Buyer].

2 Words and expressions in this Variation shall have the meanings given to them in the Contract.

3 The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature:

Date:

Name (in capitals):

Job Title:

Address:

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature:

Date:

Name (in capitals):

Job Title:

Address:

Joint Schedule 3 (Insurance Requirements)

1 The insurance the Supplier needs to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under a Call-Off Contract (specified in the applicable Order Form) ("Additional Insurances") and any other insurances as may be required by applicable Law (together the “Insurances”). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the Framework Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Call-Off Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for the Contract Period and for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

2 How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other evidence of placing cover representing any of the Insurances to which it is a party.

3 What happens if the Supplier is not insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

4 Evidence of insurance to be provided

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

5 Required amount of insurance

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6 Cancelled insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7 Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

Annex: Required insurances

1 The Supplier shall hold the following insurance cover from the Framework Start Date in accordance with this Schedule:

1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);

1.2 public liability and products insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000); and

1.3 employers' liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Joint Schedule 5 (Corporate Social Responsibility) RM1043.8

1 What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf).

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

2 Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

3 Modern Slavery, Child Labour and Inhumane Treatment

"Modern Slavery Helpline" means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery is online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff to lodge deposits or identify papers with the employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world;

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world;

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offenses anywhere around the world;

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

4 Income Security

4.1 The Supplier shall:

4.1.1 ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 ensure all workers shall be provided with written and understandable Information about their employment conditions in respect of wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

5 Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing; 5.1.3 ensure that use of overtime used responsibly, taking into account: (a) the extent;

(b) frequency; and

(c) hours worked; by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

5.3.1 this is allowed by national law;

5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

appropriate safeguards are taken to protect the workers' health and safety; and

5.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6 Sustainability

6.1 The Supplier shall meet the applicable Government Buying Standards applicable to Deliverables which is online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-governmentbuying-standards-gbs

Joint Schedule 6 (Key Subcontractors)

1 Restrictions on certain subcontractors

1.1 The Supplier is entitled, unless the Buyer states to the contrary, to sub-contract its obligations under each Call-Off Contract to the Key Subcontractors set out in the CallOff Order Form.

1.2 Subject to Paragraph 1.1, the Supplier is entitled to sub-contract some if its obligations under a Call-Off Contract to Key Subcontractors who are specifically nominated in the Order Form.

1.3 Where during the Contract Period the Supplier wishes to enter into a new Key SubContract or replace a Key Subcontractor, it must obtain the prior written consent of the Buyer and the Supplier shall, at the time of requesting such consent, provide the Buyer with the information detailed in Paragraph 1.4. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. Where the Buyer consents to the appointment of a new Key Subcontractor then they will be added to Key Subcontractor section of the Order Form. The Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the name and details of the directors, employees, agents, consultants and contractors of the subcontractor engaged in the performance of the Supplier's obligations under the Contract. Details should include: name; role; email address; address; contract details; Worker Engagement Route – for example, employed by subcontractor; engaged via worker's intermediary e.g. PSC (i.e. a personal service company), engaged as an independent sole trader or employed by another entity in supply chain;

1.4.3 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.4 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's length" terms;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Call Off Contract Period; and

1.4.6 (where applicable) the Credit Rating Threshold (as defined in Joint Schedule 7 (Financial Distress)) of the Key Subcontractor.

1.5 If requested by CCS and/or the Buyer, within 10 Working Days, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the Framework Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

1.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the buyer can end this contract) and 10.5 (When the supplier can end the contract) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key SubContract without first seeking the written consent of CCS and the Buyer.

Joint Schedule 7 (Financial Difficulties)

1 Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	**Definition**
Credit Rating Threshold	the minimum credit rating level for the Monitored Company as set out in Annex 2;

Financial Distress Event	the occurrence or one or more of the following events: (a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; (b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects;
	(c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Company; (d) Monitored Company committing a material breach of covenant to its lenders; (e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or (f) any of the following: (i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; (ii) non-payment by the Monitored Company of any financial indebtedness; (iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or (iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Call-Off Contract;
Financial Distress Service Continuity Plan	a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with [each Call-Off] Contract in the event that a Financial Distress Event occurs;
Monitored Company	Supplier [**Guarantor**] or **any Key Subcontractor**]; and
Rating Agencies	the rating agencies listed in Annex 1.

2 When this Schedule applies

2.1 The Parties shall comply with the provisions of this Schedule in relation to the assessment of the financial standing of the Monitored Companies and the consequences of a change to that financial standing.

2.2 The terms of this Schedule shall survive:

2.2.1 under the Framework Contract until the later of (a) the termination or expiry of the Framework Contract or (b) the latest date of termination or expiry of any call-off contract entered into under the Framework Contract (which might be after the date of termination or expiry of the Framework Contract); and

2.2.2 under the Call-Off Contract until the termination or expiry of the Call-Off Contract.

3 What happens when your credit rating changes

3.1 The Supplier warrants and represents to CCS that as at the Start Date the long term credit ratings issued for the Monitored Companies by each of the Rating Agencies are as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within five (5) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by any Rating Agency for a Monitored Company.

3.3 If there is any downgrade credit rating issued by any Rating Agency for the Monitored Company the Supplier shall ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with sufficient working accounts to allow further validation of financial status to be undertaken.

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agencies; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS and Buyers in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if any of the Rating Agencies have rated the Monitored Company at or below the applicable Credit Rating Threshold.

4 What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 [In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.]

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where CCS or Buyers reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1 which CCS may share with Buyers) that the Financial Distress Event could impact on the continued performance of each Contract and delivery of the Deliverables in accordance with each Call-Off Contract:

(a) submit to CCS for its Approval, a draft Financial Distress Service Continuity Plan as soon as reasonably practicable (and in any event, within ten (10) Working Days of the initial notification (or awareness) of the Financial Distress Event); and

(b) provide such financial information relating to the Monitored Company as CCS may reasonably require.

4.4 If CCS does not (acting reasonably) approve the draft Financial Distress Service Continuity Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Service Continuity Plan, which shall be resubmitted to CCS within five (5) Working Days of the rejection of the first or subsequent (as the case may be) drafts. This process shall be repeated until the Financial Distress Service Continuity Plan is Approved by CCS or referred to the Dispute Resolution Procedure.

4.5 If CCS considers that the draft Financial Distress Service Continuity Plan is insufficiently detailed to be properly evaluated, will take too long to complete or will not remedy the relevant Financial Distress Event, then it may either agree a further time period for the development and agreement of the Financial Distress Service Continuity Plan or escalate any issues with the draft Financial Distress Service Continuity Plan using the Dispute Resolution Procedure.

4.6 Following Approval of the Financial Distress Service Continuity Plan by CCS, the Supplier shall:

4.6.1 on a regular basis (which shall not be less than Monthly), review the Financial Distress Service Continuity Plan and assess whether it remains adequate and up to date to ensure the continued performance each Contract and delivery of the Deliverables in accordance with each Call-Off Contract;

4.6.2 where the Financial Distress Service Continuity Plan is not adequate or up to date in accordance with Paragraph 4.6.1, submit an updated Financial Distress Service Continuity Plan to CCS for its Approval, and the provisions of Paragraphs 4.5 and 4.6 shall apply to the review and Approval process for the updated Financial Distress Service Continuity Plan; and

4.6.3 comply with the Financial Distress Service Continuity Plan (including any updated Financial Distress Service Continuity Plan).

4.7 Where the Supplier reasonably believes that the relevant Financial Distress Event (or the circumstance or matter which has caused or otherwise led to it) no longer exists, it shall notify CCS and subject to the agreement of the Parties, the Supplier may be relieved of its obligations under Paragraph 4.6.

4.8 CCS shall be able to share any information it receives from the Buyer in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5 When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

5.2 If the Contract is terminated in accordance with Paragraph 5.1, Clauses 10.6.1 and 10.6.2 of the Core Terms shall apply as if the Contract had been terminated under Clause 10.4.1.

6 What happens If your credit rating is still good

6.1 Without prejudice to the Supplier's obligations and CCS' and the Buyer's rights and remedies under Paragraph 5, if, following the occurrence of a Financial Distress Event, the Rating Agencies review and report subsequently that the credit ratings do not drop below the relevant Credit Rating Threshold, then:

6.1.1 the Supplier shall be relieved automatically of its obligations under Paragraphs 4.3 to 4.6; and

6.1.2 CCS shall not be entitled to require the Supplier to provide financial information in accordance with Paragraph 4.3.2(b).

Annex 1: Rating Agencies

Dun and Bradstreet ("D&B")

[Rating Agency 2]

Annex 2: Credit Ratings and Credit Rating Thresholds
Part 1: Current Rating

Entity	Credit rating (long term)
REDACTED TEXT under FOIA Section 40, Personal Information	

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan

Details of the Default:	[**Guidance:** Explain the Default, with clear Schedule, Clause and Paragraph references as appropriate]		
Deadline for receiving the [**Revised**] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [**CCS/Buyer**] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete rectification of Default	**[X]** Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	**[Plan Accepted] [Plan Rejected] [Revised Plan Requested]**		
Reasons for rejection (if applicable)	[**add** reasons]		
Signed by **[CCS/Buyer]**		Date:	

Joint Schedule 11 (Processing Data) RM1043.8

Definitions

1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

Term	**Definition**
Processor Personnel	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor
	engaged in the performance of its obligations under a Contract.

Status of the Controller

2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor"; (b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where the other Party is also "Controller", in respect of certain Personal Data under a Contract and shall specify in Annex 1 (Processing Personal Data) which scenario they think shall apply in each situation. **Where one Party is Controller and the other Party its Processor**

3 Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (Processing Personal Data) by the Controller.

4 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

5 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 (Processing Personal Data), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures; (c) ensure that:

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (Processing Personal Data));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

A. are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (Data protection), 15 (What you must keep confidential) and 16 (When you can share information) of the Core Terms;

B. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

C. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

D. have undergone adequate training in the use, care, protection and handling of Personal Data;

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

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

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

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is

not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

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

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

7 Subject to Paragraph 8 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or (f) becomes aware of a Personal Data Breach.

8 The Processor's obligation to notify under Paragraph 7 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.

9 Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 7 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Personal Data Breach; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

10 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

11 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

12 The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

13 Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

14 The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

15 The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data

17 In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (Processing Data).

Independent Controllers of Personal Data

18 With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

19 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

20 Where a Party has provided Personal Data to the other Party in accordance with Paragraph 18 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

21 The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract. 22 The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) where it has recorded it in Annex 1 (Processing Personal Data).

23 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24 A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

25 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract ("Request Recipient"):

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

26 Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

27 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (Processing Personal Data).

28 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (Processing Personal Data).

29 Notwithstanding the general application of Paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal

obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 18 to 28 of this Joint Schedule 11.

Annex 2: Joint Controller Agreement

1 Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of Paragraphs 3-16 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and Paragraphs 18-28 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the **[Supplier/Relevant Authority]:**

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

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

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

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

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

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

2 Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

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

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

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

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

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

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

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

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

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

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

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

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

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

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

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

(i) nature of the data to be protected;

(ii) harm that might result from a Personal Data Breach;

(iii) state of technological development; and

(iv) cost of implementing any measures;

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

(j) ensure that it notifies the other Party as soon as it becomes aware of a Personal Data Breach.

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

3 Data Protection Breach

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

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and (b) all reasonable assistance, including:

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

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

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

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

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

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

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

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

(e) measures taken or proposed to be taken to address the Personal Data Breach; and (f) describe the likely consequences of the Personal Data Breach.

4 Audit

4.1 The Supplier shall permit:

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

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

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

5 Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

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

6 ICO Guidance

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

7 Liabilities for Data Protection Breach

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

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

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

request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (Resolving disputes).

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

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

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

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

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

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

8 Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Controller Agreement), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 of the Core Terms (Ending the contract).

9 Sub-Processing

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

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

provide evidence of such due diligence to the other Party where reasonably requested; and

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

10 **Data Retention**

The Parties agree to erase Personal Data from any computers, storage devices and storage

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