

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

Order Form

CALL-OFF REFERENCE: P5955

CALL-OFF TITLE: Infected Blood Compensation Authority
(IBCA) Cyber and Information Security

CALL-OFF CONTRACT
DESCRIPTION: proposals to establish and provide an effective CISO
function that includes security and information risk advice & management

THE BUYER: Infected Blood Compensation Authority

BUYER ADDRESS: Benton Park View, Newcastle

THE SUPPLIER: Actica Consulting Limited

SUPPLIER ADDRESS: 4, Stirling House, Stirling road. Guildford

REGISTRATION NUMBER: 3396854

DUNS NUMBER: 520304304

SID4GOV ID:

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 31/08/2025.

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

Crown Copyright 2021

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

The Parties intend that this Call-Off Contract will not, except for the first 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, SOW Template and Call-Off Schedules).

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

CALL-OFF LOT(S):

Lot 2

CALL-OFF INCORPORATED TERMS

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

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1 (Definitions) RM6263
3. Framework Special Terms
4. The following Schedules in equal order of precedence:
 - Joint Schedules for RM6263
 - Joint Schedule 2 (Variation Form)
 - Joint Schedule 3 (Insurance Requirements)
 - Joint Schedule 4 (Commercially Sensitive Information)
 - Joint Schedule 6 (Key Subcontractors)
 - Joint Schedule 7 (Financial Difficulties)
 - Joint Schedule 8 (Guarantee)

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

Crown Copyright 2021

- Joint Schedule 10 (Rectification Plan)
 - Joint Schedule 11 (Processing Data)
 - Joint Schedule 12 (Supply Chain Visibility) **(NOT USED)**
 - Joint Schedule 13 (Cyber Essentials)
 - Call-Off Schedules for RM6263
 - Call-Off Schedule 1 (Transparency Reports)
 - Call-Off Schedule 2 (Staff Transfer)
 - Call-Off Schedule 3 (Continuous Improvement)
 - Call-Off Schedule 5 (Pricing Details and Expenses Policy)
 - Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliveries)
 - Call-Off Schedule 7 (Key Supplier Staff)
 - Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
 - Call-Off Schedule 9 (Security)**removed and replaced with Annex A security schedule**
 - Call-Off Schedule 10 (Exit Management)
 - Call-off Schedule 12 (Clustering) **NOT USED**
 - Call-Off Schedule 13 (Implementation Plan and Testing)
 - Call- off Schedule 14B (Service Levels and Balancing Scorecard)
 - Call-off Schedule 15 (Call-off Contract Management)
 - Call-Off Schedule 16 (Benchmarking)**NOT USED**
 - Call-off Schedule 17 (MOD Terms) **NOT USED**
 - Call-Off Schedule 18 (Background Checks)
 - Call-Off Schedule 19 (Scottish Law) **NOT USED**
 - Call-Off Schedule 20 (Call-Off Specification)
 - Call-Off Schedule 21 (Northern Ireland Law) **NOT USED**
 - Call-Off Schedule 23 (HMRC Terms) **NOT USED**
 - Call-Off Schedule 25 (Ethical Walls Agreement)
 - Call-Off Schedule 26 (Secondment Agreement Template) **NOT USED**
5. CCS Core Terms (version 3.0.11)
 6. Joint Schedule 5 (Corporate Social Responsibility) RM6263
 7. 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:
removal of Call-Off Schedule 9 and replaced with Security Schedule Annex A developer schedule

CALL-OFF START DATE:	31/08/2025
CALL-OFF EXPIRY DATE:	30/08/2026
CALL-OFF INITIAL PERIOD:	12 Months
CALL-OFF OPTIONAL EXTENSION PERIOD:	2 X 6 months
MINIMUM NOTICE PERIOD FOR EXTENSION(S):	1 Month
CALL-OFF CONTRACT VALUE:	£1,000,000
KEY SUB-CONTRACT PRICE:	N/A

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

BUYER'S STANDARDS

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

CYBER ESSENTIALS SCHEME

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

MAXIMUM LIABILITY

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 £1,000,000 Estimated Charges in the first 12 Months of the Contract.

CALL-OFF CHARGES

- (1) Capped Time and Materials (CTM);
- (2) Incremental Fixed Price;
- (3) Time and Materials (T&M);
- (4) Fixed Price; or
- (5) A combination of two or more of the above Charging methods.

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

REIMBURSABLE EXPENSES

None

PAYMENT METHOD

Monthly in arrears

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

BUYER'S INVOICE ADDRESS: **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

All invoices must contain a valid PO number

BUYER'S AUTHORISED REPRESENTATIVE

REDACTED TEXT under FOIA Section 40, Personal Information

BUYER'S ENVIRONMENTAL POLICY

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

BUYER'S SECURITY POLICY REDACTED TEXT under FOIA Section 43 (2), Commercial 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

Quarterly on the first Working Day of each quarter]

KEY STAFF

REDACTED TEXT under FOIA Section 40, Personal Information

KEY SUBCONTRACTOR(S)

The Supplier must ensure all Supplier Staff, including any Key Sub Contractor Staff or Sub Contractor Staff are as a minimum SC checked before commencing any work under this Contract

COMMERCIALLY SENSITIVE INFORMATION

Supplier's Commercially Sensitive Information detailed in Schedule 5 and Schedule 20

BALANCED SCORECARD

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

MATERIAL KPIs

The following Material KPIs shall apply to this Call-Off Contract in accordance with Call-Off Schedule 14B (Service Levels and Balanced Scorecard): **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

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.

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:		Date:	

Appendix 1

[Insert] 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 Order Form in Framework Schedule 6 (Order Form Template, Statement of Work Template and Call-Off Schedules)).

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

Annex 1 (Template Statement of Work)

1. STATEMENT OF WORK ("SOW") DETAILS	
<p>Upon execution, this SOW forms part of the Call-Off Contract (reference below).</p> <p>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.</p> <p>All SOWs must fall within the Specification and provisions of the Call-Off Contract.</p> <p>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.</p>	
Date of SOW:	
SOW Title:	
SOW Reference:	

Call-Off Contract Reference:	
Buyer:	
Supplier:	
SOW Start Date:	
SOW End Date:	
Duration of SOW:	
Key Personnel (Buyer)	
Key Personnel (Supplier)	
Subcontractors	

2. CALL-OFF CONTRACT SPECIFICATION - PROGRAMME CONTEXT	
SOW Deliverables Background	<i>[Insert details of which elements of the Deliverables this SOW will address].</i>
Delivery phase(s)	<i>[Insert item and nature of Delivery phase(s), for example, Discovery, Alpha, Beta or Live].</i>
Overview of Requirement	<i>[Insert details including Release Types(s), for example, Adhoc, Inception, Calibration or Delivery].</i>
Accountability Models	<p><i>Please tick the Accountability Model(s) that shall be used under this Statement of Work:</i></p> <p><i>Sole Responsibility:</i> <input type="checkbox"/></p> <p><i>Self Directed Team:</i> <input type="checkbox"/></p> <p><i>Rainbow Team:</i> <input type="checkbox"/></p>

3. BUYER REQUIREMENTS – SOW DELIVERABLES			
Outcome Description			
Milestone Ref	Milestone Description	Acceptance Criteria	Due date

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

Crown Copyright 2021

MS01																		
MS02																		
Delivery Plan																		
Dependencies																		
Supplier Resource Plan																		
Security Applicable to SOW:	<p>The Supplier confirms that all Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables, have completed Supplier Staff Vetting in accordance with Paragraph 6 (Security of Supplier Staff) of Part B – Annex 1 (Baseline Security Requirements) of Call-Off Schedule 9 (Security).</p> <p>[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: <i>[insert if necessary]</i>]</p>																	
Cyber Essentials Scheme	<p>The Buyer requires the Supplier to have and maintain a Cyber Essentials Plus Certificate for the work undertaken under this SOW, in accordance with Joint Schedule 13 (Cyber Essentials Scheme).</p>																	
SOW Standards	<p><i>[Insert]</i> any specific Standards applicable to this SOW (check Annex 3 of Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules))</p>																	
Performance Management	<p><i>[Insert]</i> details of Material KPIs that have a material impact on Contract performance]</p> <table border="1"> <thead> <tr> <th>Material KPIs</th><th>Target</th><th>Measured by</th></tr> </thead> <tbody> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> </tbody> </table> <p><i>[Insert]</i> Service Levels and/or KPIs – See Call-Off Schedule 14 (Service Levels and Balanced Scorecard)]</p>			Material KPIs	Target	Measured by												
Material KPIs	Target	Measured by																
Additional Requirements	<p>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.</p>																	
Key Supplier Staff	<table border="1"> <thead> <tr> <th>Key Role</th><th>Key Staff</th><th>Contract Details</th></tr> </thead> <tbody> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td></tr> </tbody> </table> <p><i>[Indicate]</i> whether there is any requirement to issue a Status Determination Statement]</p>			Key Role	Key Staff	Contract Details												
Key Role	Key Staff	Contract Details																

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

Crown Copyright 2021

Worker Engagement Status	[Yes / No] [Insert details]														
[SOW Reporting Requirements:]	<p>[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:</p> <table border="1"> <thead> <tr> <th>Ref.</th> <th>Type of Information</th> <th>Which Services does this requirement apply to?</th> <th>Required regularity of Submission</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td>[insert]</td> <td></td> <td></td> </tr> <tr> <td>1.1</td> <td>[insert]</td> <td>[insert]</td> <td>[insert]</td> </tr> </tbody> </table> <p>1</p>			Ref.	Type of Information	Which Services does this requirement apply to?	Required regularity of Submission	1.	[insert]			1.1	[insert]	[insert]	[insert]
Ref.	Type of Information	Which Services does this requirement apply to?	Required regularity of Submission												
1.	[insert]														
1.1	[insert]	[insert]	[insert]												

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

5. SIGNATURES AND APPROVALS
<p>Agreement of this SOW</p> <p>BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the</p>

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

Crown Copyright 2021

Order Form and incorporated into the Call-Off Contract and be legally binding on the Parties:		
For and on behalf of the Supplier	Name and title	
	Date	
	Signature	
For and on behalf of the Buyer	Name and title	
	Date	
	Signature	

ANNEX 1

Data Processing

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

[TEMPLATE ANNEX 1 OF JOINT SCHEDULE 11 (PROCESSING DATA BELOW)]

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> [Insert] the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Relevant Authority] <p>The Supplier is Controller and the Relevant Authority is Processor</p> <p>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:</p> <ul style="list-style-type: none"> [Insert] the scope of Personal Data which the purposes and means of the Processing by the Relevant Authority is determined by the Supplier] <p>The Parties are Joint Controllers</p> <p>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> [Insert] the scope of Personal Data which the purposes and means of the Processing is determined by the both Parties together] <p>The Parties are Independent Controllers of Personal Data</p> <p>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</p> <ul style="list-style-type: none"> Business contact details of Supplier Personnel for which the Supplier is the Controller, Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller, [Insert] the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1)

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2021

	<p><i>the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Relevant Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Relevant Authority]</i></p> <p>[Guidance] where multiple relationships have been identified above, please address the below rows in the table for in respect of each relationship identified]</p>
Duration of the Processing	<p><i>[Clearly set out the duration of the Processing including dates]</i></p>
Nature and purposes of the Processing	<p><i>[Please be as specific as possible, but make sure that you cover all intended purposes.</i></p> <p><i>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.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]</i></p>
Type of Personal Data	<p><i>[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]</i></p>
Categories of Data Subject	<p><i>[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.]</i></p>
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	<p><i>[Describe how long the data will be retained for, how it be returned or destroyed]</i></p>

Call-Off Schedule 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-note->

Framework Ref: RM6263

Project Version: v1.0

Model Version: v3.0

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2021

[0117-update-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.

Call-Off Schedule 1 (Transparency Reports)

Call-Off Ref:

Crown Copyright 2021

Annex A: List of Transparency Reports

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

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Call-Off Schedule 2 (Staff Transfer)

1. Definitions

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

"Employee Liability"	<p>1 all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:</p> <ul style="list-style-type: none">a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;b) unfair, wrongful or constructive dismissal compensation;c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;d) compensation for less favourable treatment of part-time workers or fixed term employees;e) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Subcontractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;f) claims whether in tort, contract or statute or otherwise; <p>any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation;</p>
-----------------------------	---

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

"Former Supplier"	a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Deliverables (or any part of the Deliverables) and shall include any Subcontractor of
--------------------------	---

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

	such supplier (or any Subcontractor of any such Subcontractor);
"Partial Termination"	the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract) or 10.6 (When the Supplier can end the contract);
"Relevant Transfer"	a transfer of employment to which the Employment Regulations applies;
"Relevant Transfer Date"	in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate;
"Supplier's Final Supplier Personnel List"	a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date;
"Supplier's Provisional Supplier Personnel List"	a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

"Staffing Information"	<p>in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format:</p> <ul style="list-style-type: none">(a) their ages, dates of commencement of employment or engagement, gender and place of work;(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;(c) the identity of the employer or relevant contracting Party;(d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;(e) their wages, salaries, bonuses and profit sharing arrangements as applicable;(f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;(g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);(h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;(i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and(j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations;
-------------------------------	---

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

"Term"	the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract;
"Transferring Buyer Employees"	those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date;
"Transferring Former Supplier Employees"	in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date.

2. INTERPRETATION

Where a provision in this Schedule imposes any obligation on the Supplier including (without limit) to comply with a requirement or provide an indemnity, undertaking or warranty, the Supplier shall procure that each of its Subcontractors shall comply with such obligation and provide such indemnity, undertaking or warranty to CCS, the Buyer, Former Supplier, Replacement Supplier or Replacement Subcontractor, as the case maybe and where the Subcontractor fails to satisfy any claims under such indemnities the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

3. Which parts of this Schedule apply

Only the:

- 3.1 parts of this Schedule identified in the Order Form shall apply to this Call-Off Contract; or
- 3.2 following parts of this Schedule shall apply to this Call-Off Contract:

[Delete if not applicable to the Call-Off Contract]

- o [Part A (Staff Transfer At Start Date – Outsourcing From the Buyer)]
- o [Part B (Staff Transfer At Start Date – Transfer From Former Supplier)]
- o [Part C (No Staff Transfer On Start Date)]
- o [Part D (Pensions)]
 - o [- Annex D1 (CSPS)]
 - o [- Annex D2 (NHSPS)]
 - o [- Annex D3 (LGPS)]
 - o [- Annex D4 (Other Schemes)]
- o [Part E (Staff Transfer on Exit)]

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

1. PART A: STAFF TRANSFER AT THE START DATE

2. OUTSOURCING FROM THE BUYER

1. What is a relevant transfer

1.1 The Buyer and the Supplier agree that:

- 1.1.1 the commencement of the provision of the Services or of each relevant part of the Services will be a Relevant Transfer in relation to the Transferring Buyer Employees; and
- 1.1.2 as a result of the operation of the Employment Regulations, the contracts of employment between the Buyer and the Transferring Buyer Employees (except in relation to any terms disapplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Subcontractor and each such Transferring Buyer Employee.
- 1.1.3 The Buyer shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Buyer Employees in respect of the period arising up to (but not including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions.

2. Indemnities the Buyer must give

- 2.1 Subject to Paragraph 2.2, the Buyer shall indemnify the Supplier and any Sub-Contractor against any Employee Liabilities arising from or as a result of any act or omission by the indemnifying party in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee occurring before the Relevant Transfer Date.
- 2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Subcontractor whether occurring or having its origin before, on or after the Relevant Transfer Date.
- 2.3 Subject to Paragraphs 2.4 and 2.5, if any employee of the Buyer who is not identified as a Transferring Buyer Employee claims, or it is determined in relation to any employees of the Buyer, that his/her contract of employment has been transferred from the Buyer to the Supplier and/or any Subcontractor pursuant to the Employment Regulations then -
 - 2.3.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;
 - 2.3.2 the Buyer may offer employment to such person, or take such other steps as it considers appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 2.3.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;
- 2.3.4 if after the period referred to in Paragraph 2.3.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 2.3.1 to 2.3.4 the Buyer will indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in this Paragraph 2.3.

2.4 The indemnity in Paragraph 2.3 shall not apply to any claim:

- 2.4.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or any Subcontractor; or
- 2.4.2 any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure.

2.5 The indemnity in Paragraph 2.3 shall not apply to any termination of employment occurring later than 3 Months from the Relevant Transfer Date.

2.6 If the Supplier and/or any Subcontractor at any point accept the employment of any person as is described in Paragraph 2.3, such person shall be treated as having transferred to the Supplier and/or any Subcontractor and the Supplier shall comply with such obligations as may be imposed upon it under applicable Law.

3. Indemnities the Supplier must give and its obligations

3.1 Subject to Paragraph 3.2, the Supplier shall indemnify the Buyer against any Employee Liabilities arising from or as a result of any act or omission by the Supplier or any Subcontractor in respect of any Transferring Buyer Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Buyer Employee whether occurring before, on or after the Relevant Transfer Date.

3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Buyer whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Buyer's failure to comply with its obligations under the Employment Regulations.

3.3 The Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of the Transferring Buyer Employees, from (and including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

insurance contributions and pension contributions and any other sums due under Part D: Pensions.

4. Information the Supplier must provide

The Supplier shall promptly provide to the Buyer in writing such information as is necessary to enable the Buyer to carry out its duties under regulation 13 of the Employment Regulations. The Buyer shall promptly provide to the Supplier in writing such information as is necessary to enable the Supplier and any Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.

5. Cabinet Office requirements

- 5.1 The Parties agree that the Principles of Good Employment Practice issued by the Cabinet Office in December 2010 apply to the treatment by the Supplier of employees whose employment begins after the Relevant Transfer Date, and the Supplier undertakes to treat such employees in accordance with the provisions of the Principles of Good Employment Practice.
- 5.2 The Supplier shall comply with any requirement notified to it by the Buyer relating to pensions in respect of any Transferring Buyer Employee as set down in (i) the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised 2007; (ii) HM Treasury's guidance "Staff Transfers from Central Government: A Fair Deal for Staff Pensions of 1999; (iii) HM Treasury's guidance "Fair deal for staff pensions: procurement of Bulk Transfer Agreements and Related Issues" of June 2004; and/or (iv) the New Fair Deal.
- 5.3 Any changes embodied in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraphs 5.1 or 5.2 shall be agreed in accordance with the Variation Procedure.

6. Pensions

- 6.1 The Supplier shall comply with:
 - 6.1.1 all statutory pension obligations in respect of all Transferring Buyer Employees; and
 - 6.1.2 the provisions in Part D: Pensions.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

3. PART B: STAFF TRANSFER AT THE START DATE

4. TRANSFER FROM A FORMER SUPPLIER ON RE-PROCUREMENT

1. What is a relevant transfer

1.1 The Buyer and the Supplier agree that:

1.1.1 the commencement of the provision of the Services or of any relevant part of the Services will be a Relevant Transfer in relation to the Transferring Former Supplier Employees; and

1.1.2 as a result of the operation of the Employment Regulations, the contracts of employment between each Former Supplier and the Transferring Former Supplier Employees (except in relation to any terms disapplied through the operation of regulation 10(2) of the Employment Regulations) shall have effect on and from the Relevant Transfer Date as if originally made between the Supplier and/or any Subcontractor and each such Transferring Former Supplier Employee.

1.2 The Buyer shall procure that each Former Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees in respect of the period up to (but not including) the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions.

2. Indemnities given by the Former Supplier

2.1 Subject to Paragraph 2.2, the Buyer shall procure that each Former Supplier shall indemnify the Supplier and any Subcontractor against any Employee Liabilities arising from or as a result of any act or omission by the Former Supplier in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee arising before the Relevant Transfer Date;

2.2 The indemnities in Paragraph 2.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier or any Subcontractor whether occurring or having its origin before, on or after the Relevant Transfer Date.

2.3 Subject to Paragraphs 2.4 and 2.5, if any employee of a Former Supplier who is not identified as a Transferring Former Supplier Employee and claims, and/or it is determined, in relation to such person that his/her contract of employment has been transferred from a Former Supplier to the Supplier and/or any Notified Subcontractor pursuant to the Employment Regulations then:

2.3.1 the Supplier will within 5 Working Days of becoming aware of that fact notify the Buyer and the relevant Former Supplier in writing;

2.3.2 the Former Supplier may offer employment to such person, or take such other steps as it considers appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 2.3.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;
 - 2.3.4 if after the period referred to in Paragraph 2.3.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;
- 1. and subject to the Supplier's compliance with Paragraphs 2.3.1 to 2.3.4 the Buyer shall procure that the Former Supplier will indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Former Supplier's employees referred to in paragraph 2.3.
- 2.4 The indemnity in Paragraph 2.3 shall not apply to any claim:
 - 2.4.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Supplier and/or any Subcontractor; or
 - 2.4.2 that the termination of employment was unfair because the Supplier and/or Subcontractor neglected to follow a fair dismissal procedure.
- 2.5 The indemnity in Paragraph 2.3 shall not apply to any termination of employment occurring later than 3 Months from the Relevant Transfer Date.
- 2.6 If the Supplier and/or any Subcontractor at any point accept the employment of any person as is described in Paragraph 2.3, such person shall be treated as having transferred to the Supplier and/or any Subcontractor and the Supplier shall comply with such obligations as may be imposed upon it under applicable Law.
- 3. Indemnities the Supplier must give and its obligations**
 - 3.1 Subject to Paragraph 3.1, the Supplier shall indemnify the Buyer, and the Former Supplier against any Employee Liabilities arising from or as a result of any act or omission by the Supplier or any Subcontractor in respect of any Transferring Former Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Former Supplier Employee whether occurring before, on or after the Relevant Transfer Date.
 - 3.2 The indemnities in Paragraph 3.1 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Former Supplier whether occurring or having its origin before, on or after the Relevant Transfer Date including, without limitation, any Employee Liabilities arising from the Former Supplier's failure to comply with its obligations under the Employment Regulations.
 - 3.3 The Supplier shall comply with all its obligations under the Employment Regulations and shall perform and discharge all its obligations in respect of all the Transferring Former Supplier Employees, on and from the Relevant Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

insurance contributions and pension contributions and all such sums due under Part D: Pensions.

4. Information the Supplier must give

The Supplier shall promptly provide to the Buyer and/or at the Buyer's direction, the Former Supplier, in writing such information as is necessary to enable the Buyer and/or the Former Supplier to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Former Supplier shall promptly provide to the Supplier in writing such information as is necessary to enable the Supplier and any Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.

5. Cabinet Office requirements

- 5.1 The Supplier shall comply with any requirement notified to it by the Buyer relating to pensions in respect of any Transferring Former Supplier Employee as set down in (i) the Cabinet Office Statement of Practice on Staff Transfers in the Public Sector of January 2000, revised 2007; (ii) HM Treasury's guidance "Staff Transfers from Central Government: A Fair Deal for Staff Pensions of 1999; (iii) HM Treasury's guidance: "Fair deal for staff pensions: procurement of Bulk Transfer Agreements and Related Issues" of June 2004; and/or (iv) the New Fair Deal.
- 5.2 Any changes embodied in any statement of practice, paper or other guidance that replaces any of the documentation referred to in Paragraph 5.1 shall be agreed in accordance with the Change Control Procedure.

6. Limits on the Former Supplier's obligations

Notwithstanding any other provisions of this Part B, where in this Part B the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer's must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

7. Pensions

- 7.1 The Supplier shall comply with:
 - 7.1.1 all statutory pension obligations in respect of all Transferring Former Supplier Employees; and
 - 7.1.2 the provisions in Part D: Pensions.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

PART C: NO STAFF TRANSFER ON THE START DATE

1. What happens if there is a staff transfer

- 1.1 The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.
- 1.2 Subject to Paragraphs 1.3, 1.4 and 1.5, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Subcontractor pursuant to the Employment Regulations then:
 - 1.2.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;
 - 1.2.2 the Buyer may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Supplier;
 - 1.2.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;
 - 1.2.4 if after the period referred to in paragraph 1.2.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;and subject to the Supplier's compliance with Paragraphs 1.2.1 to 1.2.4:
 - (a) the Buyer will indemnify the Supplier and/or the relevant Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 1.2; and
 - (b) the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Subcontractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 1.2.
- 1.3 The indemnities in Paragraph 1.2 shall not apply to any claim:
 - 1.3.1 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Subcontractor; or
 - 1.3.2 any claim that the termination of employment was unfair because the Supplier and/or any Subcontractor neglected to follow a fair dismissal procedure

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 1.4 The indemnities in Paragraph 1.2 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.
- 1.5 If the Supplier and/or the Subcontractor does not comply with Paragraph 1.2, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Subcontractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Subcontractor.

2. Limits on the Former Supplier's obligations

Where in this Part C the Buyer accepts an obligation to procure that a Former Supplier does or does not do something, such obligation shall be limited so that it extends only to the extent that the Buyer's contract with the Former Supplier contains a contractual right in that regard which the Buyer may enforce, or otherwise so that it requires only that the Buyer must use reasonable endeavours to procure that the Former Supplier does or does not act accordingly.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

5. PART D: PENSIONS

1. Definitions

In this Part D, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions), and shall be deemed to include the definitions set out in the Annexes:

"Actuary"	a Fellow of the Institute and Faculty of Actuaries;
"Admission Agreement"	means either or both of the CSPA Admission Agreement (as defined in Annex D1: CSPA) or the LGPS Admission Agreement) as defined in Annex D3: LGPS), as the context requires;
"Broadly Comparable"	<p>(a) in respect of a pension scheme, a status satisfying the condition that there are no identifiable employees who will suffer material detriment overall in terms of future accrual of pension benefits as assessed in accordance with Annex A of New Fair Deal and demonstrated by the issue by the Government Actuary's Department of a broad comparability certificate; and</p> <p>(b) in respect of benefits provided for or in respect of a member under a pension scheme, benefits that are consistent with that pension scheme's certificate of broad comparability issued by the Government Actuary's Department,</p> <p>and "Broad Comparability" shall be construed accordingly;</p>
"CSPA"	the schemes as defined in Annex D1 to this Part D;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

"Fair Deal Employees"	<p>those:</p> <ul style="list-style-type: none"> (a) Transferring Buyer Employees; and/or (b) Transferring Former Supplier Employees; and/or (c) employees who are not Transferring Buyer Employees or Transferring Former Supplier Employees but to whom the Employment Regulations apply on the Relevant Transfer Date to transfer their employment to the Supplier or a Subcontractor, and whose employment is not terminated in accordance with the provisions of Paragraphs 2.3.4 of Parts A or B or Paragraph 1.2.4 of Part C; (d) where the Former Supplier becomes the Supplier those employees; <p>who at the Commencement Date or Relevant Transfer Date (as appropriate) are or become entitled to New Fair Deal protection in respect of any of the Statutory Schemes as notified by the Buyer;</p>
"Fair Deal Schemes"	means the relevant Statutory Scheme or a Broadly Comparable pension scheme;
"Fund Actuary"	means Fund Actuary as defined in Annex D3 to this Part D;
"LGPS"	the schemes as defined in Annex D3 to this Part D;
"NHSPS"	the schemes as defined in Annex D2 to this Part D;
"New Fair Deal"	<p>the revised Fair Deal position set out in the HM Treasury guidance: <i>"Fair Deal for Staff Pensions: Staff Transfer from Central Government"</i> issued in October 2013 including:</p> <ul style="list-style-type: none"> (a) any amendments to that document immediately prior to the Relevant Transfer Date; and (b) any similar pension protection in accordance with the subsequent Annex D1-D3 inclusive as notified to the Supplier by the CCS or Buyer; and
"Statutory Schemes"	means the CSPA, NHSPS or LGPS.

2. Supplier obligations to participate in the pension schemes

2.1 In respect of all or any Fair Deal Employees each of Annex D1: CSPA, Annex D2: NHSPS and/or Annex D3: LGPS shall apply, as appropriate.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

2.2 The Supplier undertakes to do all such things and execute any documents (including any relevant Admission Agreement and/or Direction Letter, if necessary) as may be required to enable the Supplier to participate in the appropriate Statutory Scheme in respect of the Fair Deal Employees and shall bear its own costs in such regard.

2.3 The Supplier undertakes:

2.3.1 to pay to the Statutory Schemes all such amounts as are due under the relevant Admission Agreement and/or Direction Letter or otherwise and shall deduct and pay to the Statutory Schemes such employee contributions as are required; and

2.3.2 to be fully responsible for all other costs, contributions, payments and other amounts relating to its participation in the Statutory Schemes, including for the avoidance of doubt any exit payments and the costs of providing any bond, indemnity or guarantee required in relation to such participation.

3. Supplier obligation to provide information

3.1 The Supplier undertakes to the Buyer:

3.1.1 to provide all information which the Buyer may reasonably request concerning matters referred to in this Part D as expeditiously as possible; and

3.1.2 not to issue any announcements to any Fair Deal Employee prior to the Relevant Transfer Date concerning the matters stated in this Part D without the consent in writing of the Buyer (such consent not to be unreasonably withheld or delayed).

4. Indemnities the Supplier must give

4.1 The Supplier undertakes to the Buyer to indemnify and keep indemnified CCS, NHS Pensions the Buyer and/or any Replacement Supplier and/or any Replacement Subcontractor on demand from and against all and any Losses whatsoever arising out of or in connection with any liability towards all and any Fair Deal Employees arising in respect of service on or after the Relevant Transfer Date which arise from any breach by the Supplier of this Part D, and/or the CSPA Admission Agreement and/or the Direction Letter and/or the LGPS Admission Agreement or relates to the payment of benefits under and/or participation in an occupational pension scheme (within the meaning provided for in section 1 of the Pension Schemes Act 1993) or the Fair Deal Schemes.

4.2 The Supplier hereby indemnifies the CCS, NHS Pensions, the Buyer and/or any Replacement Supplier and/or Replacement Subcontractor from and against all Losses suffered or incurred by it or them which arise from claims by Fair Deal Employees of the Supplier and/or of any Subcontractor or by any trade unions, elected employee representatives or staff associations in respect of all or any such Fair Deal Employees which Losses:

4.2.1 relate to pension rights in respect of periods of employment on and after the Relevant Transfer Date until the date of termination or expiry of this Contract; or

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 4.2.2 arise out of the failure of the Supplier and/or any relevant Subcontractor to comply with the provisions of this Part D before the date of termination or expiry of this Contract.

4.3 The indemnities in this Part D and its Annexes:

- 4.3.1 shall survive termination of this Contract; and
- 4.3.2 shall not be affected by the caps on liability contained in Clause 11 (How much you can be held responsible for).

5. What happens if there is a dispute

5.1 The Dispute Resolution Procedure will not apply to this Part D and any dispute between the CCS and/or the Buyer and/or the Supplier or between their respective actuaries or the Fund Actuary about any of the actuarial matters referred to in this Part D and its Annexes shall in the absence of agreement between the CCS and/or the Buyer and/or the Supplier be referred to an independent Actuary:

- 5.1.1 who will act as an expert and not as an arbitrator;
- 5.1.2 whose decision will be final and binding on the CCS and/or the Buyer and/or the Supplier; and
- 5.1.3 whose expenses shall be borne equally by the CCS and/or the Buyer and/or the Supplier unless the independent Actuary shall otherwise direct.

6. Other people's rights

- 6.1 The Parties agree Clause 19 (Other people's rights in this contract) does not apply and that the CRTPA applies to this Part D to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to him or her or it by the Supplier under this Part D, in his or her or its own right under section 1(1) of the CRTPA.
- 6.2 Further, the Supplier must ensure that the CRTPA will apply to any Sub-Contract to the extent necessary to ensure that any Fair Deal Employee will have the right to enforce any obligation owed to them by the Subcontractor in his or her or its own right under section 1(1) of the CRTPA.

7. What happens if there is a breach of this Part D

- 7.1 The Supplier agrees to notify the Buyer should it breach any obligations it has under this Part D and agrees that the Buyer shall be entitled to terminate its Contract for material Default in the event that the Supplier:
 - 7.1.1 commits an irremediable breach of any provision or obligation it has under this Part D; or
 - 7.1.2 commits a breach of any provision or obligation it has under this Part D which, where capable of remedy, it fails to remedy within a reasonable time and in any event within 28 days of the date of a notice from the Buyer giving particulars of the breach and requiring the Supplier to remedy it.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

8. Transferring New Fair Deal Employees

8.1 Save on expiry or termination of this Contract, if the employment of any Fair Deal Employee transfers to another employer (by way of a transfer under the Employment Regulations) the Supplier shall and shall procure that any relevant Subcontractor shall:

- 8.1.1 consult with and inform those Fair Deal Employees of the pension provisions relating to that transfer; and
- 8.1.2 procure that the employer to which the Fair Deal Employees are transferred (the **"New Employer"**) complies with the provisions of this Part D and its Annexes provided that references to the "Supplier" will become references to the New Employer, references to "Relevant Transfer Date" will become references to the date of the transfer to the New Employer and references to "Fair Deal Employees" will become references to the Fair Deal Employees so transferred to the New Employer.

9. What happens to pensions if this Contract ends

The provisions of Part E: Staff Transfer On Exit (Mandatory) apply in relation to pension issues on expiry or termination of this Contract.

10. Broadly Comparable Pension Schemes

10.1 If either:

- 10.1.1 the terms of any of Paragraphs 2.2 of Annex D1: CSPS, 5.2 of Annex D2: NHSPS and or 4 of Annex D3: LGPS apply; and/or
- 10.1.2 the Buyer agrees, having considered the exceptional cases provided for in New Fair Deal, (such agreement not to be unreasonably withheld) that the Supplier (and/or its Subcontractors, if any) need not continue to provide the Fair Deal Employees, who continue to qualify for Fair Deal Protection, with access to the appropriate Statutory Scheme;

the Supplier must (and must, where relevant, procure that each of its Subcontractors will) ensure that, with effect from the Relevant Transfer Date or if later cessation of participation in the Statutory Scheme until the day before the Service Transfer Date, the relevant Fair Deal Employees will be eligible for membership of a pension scheme under which the benefits are Broadly Comparable to those provided under the relevant Statutory Scheme, and then on such terms as may be decided by the Buyer.

10.2 Where the Supplier has set up a Broadly Comparable pension scheme or schemes pursuant to the provisions of Paragraph 10.1, the Supplier shall (and shall procure that any of its Subcontractors shall):

- 10.2.1 supply to the Buyer details of its (or its Subcontractor's) Broadly Comparable pension scheme and provide a full copy of the valid certificate of broad comparability covering all relevant Fair Deal

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- Employees, as soon as it is able to do so and in any event no later than 28 days before the Relevant Transfer Date;
- 10.2.2 fully fund any such Broadly Comparable pension scheme in accordance with the funding requirements set by that Broadly Comparable pension scheme's Actuary or by the Government Actuary's Department for the period ending on the Service Transfer Date;
- 10.2.3 instruct any such Broadly Comparable pension scheme's Actuary to, and to provide all such co-operation and assistance in respect of any such Broadly Comparable pension scheme as the Replacement Supplier and/or CCS and/or NHS Pension and/or CSPA and/or the relevant Administering Authority and/or the Buyer may reasonably require, to enable the Replacement Supplier to participate in the appropriate Statutory Scheme in respect of any Fair Deal Employee that remain eligible for New Fair Deal protection following a Service Transfer;
- 10.2.4 provide a replacement Broadly Comparable pension scheme with immediate effect for those Fair Deal Employees who are still employed by the Supplier and/or relevant Subcontractor and are still eligible for New Fair Deal protection in the event that the Supplier and/or Subcontractor's Broadly Comparable pension scheme is terminated;
- 10.2.5 allow and make all necessary arrangements to effect, in respect of any Fair Deal Employee that remains eligible for New Fair Deal protection, following a Service Transfer, the bulk transfer of past service from any such Broadly Comparable pension scheme into the relevant Statutory Scheme and as is relevant on a day for day service basis and to give effect to any transfer of accrued rights required as part of participation under New Fair Deal. For the avoidance of doubt, should the amount offered by the Broadly Comparable pension scheme be less than the amount required by the appropriate Statutory Scheme to fund day for day service ("**Shortfall**"), the Supplier or the Subcontractor (as agreed between them) must pay the Statutory Scheme, as required, provided that in the absence of any agreement between the Supplier and any Subcontractor, the Shortfall shall be paid by the Supplier; and
- 10.2.6 indemnify CCS and/or the Buyer and/or NHS Pension and/or CSPA and/or the relevant Administering Authority and/or on demand for any failure to pay the Shortfall as required under Paragraph 10.2.5 above.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Annex D1:

Civil Service Pensions Schemes (CSPS)

1. Definitions

In this Annex D1: CSPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"CSPS Admission Agreement"	an admission agreement in the form available on the Civil Service Pensions website immediately prior to the Relevant Transfer Date to be entered into for the CSPS in respect of the Services;
"CSPS Eligible Employee"	any Fair Deal Employee who at the relevant time is an eligible employee as defined in the CSPS Admission Agreement;
"CSPS"	the Principal Civil Service Pension Scheme available to Civil Servants and employees of bodies under Schedule 1 of the Superannuation Act 1972 (and eligible employees of other bodies admitted to participate under a determination under section 25 of the Public Service Pensions Act 2013), as governed by rules adopted by Parliament; the Partnership Pension Account and its (i) Ill health Benefits Arrangements and (ii) Death Benefits Arrangements; the Civil Service Additional Voluntary Contribution Scheme; after 30 September 2018: the Designated Stakeholder Pension Scheme which is scheduled to close to new members in September 2018] and "alpha" introduced under The Public Service (Civil Servants and Others) Pensions Regulations 2014.

2. Access to equivalent pension schemes after transfer

- 2.1 The Supplier shall procure that the Fair Deal Employees, shall be either admitted into, or offered continued membership of, the relevant section of the CSPS that they currently contribute to, or were eligible to join immediately prior to the Relevant Transfer Date or became eligible to join on the Relevant Transfer Date and the Supplier shall procure that the Fair Deal Employees continue to accrue benefits in accordance with the provisions governing the relevant section of the CSPS for service from (and including) the Relevant Transfer Date.
- 2.2 The Supplier undertakes that should it cease to participate in the CSPS for whatever reason at a time when it has CSPS Eligible Employees, that it will, at no extra cost to the Buyer, provide to any Fair Deal Employee who immediately prior to such cessation of participation remained a CSPS Eligible Employee with access to a pension scheme which is Broadly Comparable to the CSPS on the date the CSPS Eligible Employees ceased to participate in the CSPS.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Annex D2: NHS Pension Schemes

1. Definitions

In this Annex D2: NHSPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Direction Letter"	NHS Pensions Direction or Determination (as appropriate) issued by the Secretary of State in exercise of the powers conferred by section 7 of the Superannuation (Miscellaneous Provisions) Act 1967 or by section 25 of the Public Service Pensions Act 2013 (as appropriate) and issued to the Supplier or a Subcontractor of the Supplier (as appropriate) relating to the terms of participation of the Supplier or Subcontractor in the NHSPS in respect of the NHSPS Eligible Employees;
---------------------------	--

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

NHSPS Eligible Employees"	<p>h of the Fair Deal Employees who at a Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the NHSPS as a result of either:</p> <ul style="list-style-type: none">(a) their employment with the Buyer, an NHS Body or other employer which participates automatically in the NHSPS; or(b) their employment with a Former Supplier who provides access to the NHSPS pursuant to an NHS Pensions Direction or Determination (as appropriate) issued by the Secretary of State in exercise of the powers conferred by section 7 of the Superannuation (Miscellaneous Provisions) Act 1967 or by section 25 of the Public Service Pensions Act 2013 (as appropriate) in respect of their employment with that Former Supplier (on the basis that they are entitled to protection under New Fair Deal and were permitted to re-join the NHSPS, having been formerly in employment with the Buyer, an NHS Body or other employer who participated automatically in the NHSPS in connection with the Services, prior to being employed by the Former Supplier), <p>, in each case, being continuously engaged for more than fifty per cent (50%) of their employed time in the delivery of services (the same as or similar to the Services).</p> <p>the avoidance of doubt, an individual who is in or entitled to become a member of the NHSPS as a result of being engaged in the Services and being covered by an "open" Direction Letter or other NHSPS "access" facility but who has never been employed directly by an NHS Body (or other body which participates automatically in the NHSPS) is not an NHSPS Eligible Employee;</p>
"NHS Body"	the meaning given to it in section 275 of the National Health Service Act 2006 as amended by section 138(2)(c) of Schedule 4 to the Health and Social Care Act 2012;
"NHS Pensions"	NHS Pensions as the administrators of the NHSPS or such other body as may from time to time be

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

	responsible for relevant administrative functions of the NHSPS;
"NHSPS"	National Health Service Pension Scheme for England and Wales, established pursuant to the Superannuation Act 1972 and governed by subsequent regulations under that Act including the NHS Pension Scheme Regulations;
"NHS Pension Scheme Arrears"	failure on the part of the Supplier or its Subcontractors (if any) to pay employer's contributions or deduct and pay across employee's contributions to the NHSPS or meet any other financial obligations under the NHSPS or any Direction Letter in respect of the NHSPS Eligible Employees;
"NHS Pension Scheme Regulations"	appropriate, any or all of the National Health Service Pension Scheme Regulations 1995 (SI 1995/300), the National Health Service Pension Scheme Regulations 2008 (SI 2008/653), the National Health Service Pension Scheme Regulations 2015 (2015/94) and any subsequent regulations made in respect of the NHSPS, each as amended from time to time;
"NHS Premature Retirement Rights"	its to which any Fair Deal Employee (had they remained in the employment of the Buyer, an NHS Body or other employer which participates automatically in the NHSPS) would have been or are entitled under the NHS Pension Scheme Regulations, the NHS Compensation for Premature Retirement Regulations 2002 (SI 2002/1311), the NHS (Injury Benefits) Regulations 1995 (SI 1995/866) and section 45 of the General Whitley Council conditions of service, or any other legislative or contractual provision which replaces, amends, extends or consolidates the same from time to time;
"Pension Benefits"	benefits payable in respect of an individual (including but not limited to pensions related allowances and lump sums) relating to old age, invalidity or survivor's benefits provided under an occupational pension scheme; and
"Retirement Benefits Scheme"	pension scheme registered under Chapter 2 of Part 4 of the Finance Act 2004.

2. Membership of the NHS Pension Scheme

- 2.1 In accordance with New Fair Deal, the Supplier and/or any of its Subcontractors to which the employment of any NHSPS Eligible Employee compulsorily transfers as a result of the award of this Contract, if not an NHS Body or other employer which participates automatically in the NHSPS, must by or as soon as reasonably

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

practicable after the Relevant Transfer Date, each secure a Direction Letter to enable the NHSPS Eligible Employees to retain either continuous active membership of or eligibility for, the NHSPS for so long as they remain employed in connection with the delivery of the Services under this Contract, and have a right to membership or eligibility of that scheme under the terms of the Direction Letter.

- 2.2 The Supplier must supply to the Buyer by or as soon as reasonably practicable after the Relevant Transfer Date a complete copy of each Direction Letter.
- 2.3 The Supplier must ensure (and procure that each of its Subcontractors (if any) ensures) that all of its NHSPS Eligible Employees have a contractual right to continuous active membership of or eligibility for the NHSPS for so long as they have a right to membership or eligibility of that scheme under the terms of the Direction Letter.
- 2.4 The Supplier will (and will procure that its Subcontractors (if any) will) comply with the terms of the Direction Letter, the NHS Pension Scheme Regulations (including any terms which change as a result of changes in Law) and any relevant policy issued by the Department of Health in respect of the NHSPS Eligible Employees for so long as it remains bound by the terms of any such Direction Letter.
- 2.5 Where any employee omitted from the Direction Letter supplied in accordance with Paragraph 2 of this Annex are subsequently found to be an NHSPS Eligible Employee, the Supplier will (and will procure that its Subcontractors (if any) will) treat that person as if they had been an NHSPS Eligible Employee from the Relevant Transfer Date so that their Pension Benefits and NHS Premature Retirement Rights are not adversely affected.
- 2.6 The Supplier will (and will procure that its Subcontractors (if any) will) as soon as reasonably practicable and at its (or its Subcontractor's) cost, obtain any guarantee, bond or indemnity that may from time to time be required by the Secretary of State for Health.

3. Access to NHS Pension Schemes after transfer

The Supplier will procure that with effect from the Relevant Transfer Date the NHSPS Eligible Employees shall be either eligible for or remain in continuous active membership of (as the case may be) the NHSPS for employment from (and including) the Relevant Transfer Date.

4. Continuation of early retirement rights after transfer

From the Relevant Transfer Date until the Service Transfer Date, the Supplier must provide (and/or must ensure that its Subcontractors (if any) provide) NHS Premature Retirement Rights in respect of the NHSPS Eligible Employees that are identical to the benefits they would have received had they remained employees of the Buyer, an NHS Body or other employer which participates automatically in the NHSPS.

5. What the buyer do if the Supplier breaches its pension obligations

- 5.1 The Supplier agrees that the Buyer is entitled to make arrangements with NHS Pensions for the Buyer to be notified if the Supplier (or its Subcontractor) breaches the terms of its Direction Letter. Notwithstanding the provisions of the foregoing, the

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Supplier shall notify the Buyer in the event that it (or its Subcontractor) breaches the terms of its Direction Letter.

5.2 If the Buyer is entitled to terminate the Contract or the Supplier (or its Subcontractor, if relevant) ceases to participate in the NHSPS for whatever other reason, the Buyer may in its sole discretion, and instead of exercising its right to terminate this Contract where relevant, permit the Supplier (or any such Subcontractor, as appropriate) to offer Broadly Comparable Pension Benefits, on such terms as decided by the Buyer. The provisions of Paragraph 10 (Bulk Transfer Obligations in relation to any Broadly Comparable pension scheme) of Part D: Pensions shall apply in relation to any Broadly Comparable pension scheme established by the Supplier or its Subcontractors.

5.3 In addition to the Buyer's right to terminate the Contract, if the Buyer is notified by NHS Pensions of any NHS Pension Scheme Arrears, the Buyer will be entitled to deduct all or part of those arrears from any amount due to be paid under this Contract or otherwise.

6. Compensation when pension scheme access can't be provided

6.1 If the Supplier (or its Subcontractor, if relevant) is unable to provide the NHSPS Eligible Employees with either:

6.1.1 membership of the NHSPS (having used its best endeavours to secure a Direction Letter); or

6.1.2 access to a Broadly Comparable pension scheme,

the Buyer may in its sole discretion permit the Supplier (or any of its Subcontractors) to compensate the NHSPS Eligible Employees in a manner that is Broadly Comparable or equivalent in cash terms, the Supplier (or Subcontractor as relevant) having consulted with a view to reaching agreement with any recognised trade union or, in the absence of such body, the NHSPS Eligible Employees. The Supplier must meet (or must procure that the relevant Subcontractor meets) the costs of the Buyer determining whether the level of compensation offered is reasonable in the circumstances.

6.2 This flexibility for the Buyer to allow compensation in place of Pension Benefits is in addition to and not instead of the Buyer's right to terminate the Contract.

7. Indemnities that a Supplier must give

7.1 The Supplier must indemnify and keep indemnified the CCS, the Buyer and any Replacement Supplier against all Losses arising out of any claim by any NHSPS Eligible Employee that the provision of (or failure to provide) Pension Benefits and NHS Premature Retirement Rights from the Relevant Transfer Date, or the level of such benefit provided, constitutes a breach of his or her employment rights.

7.2 The Supplier must indemnify and keep indemnified the Buyer, NHS Pensions and any Replacement Supplier against all Losses arising out of the Supplier (or its Subcontractor) allowing anyone who is not an NHSPS Eligible Employee to join or claim membership of the NHSPS at any time during the Contract Period.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

8. Subcontractors

- 8.1 If the Supplier enters into a Sub-Contract for the delivery of all or part or any component of the Services which will involve the transfer of employment of any NHSPS Eligible Employee it will impose obligations on its Subcontractor in identical terms as those imposed on the Supplier in relation to Pension Benefits and NHS Premature Retirement Rights by this Annex, including requiring that:
- 8.1.1 if the Supplier has secured a Direction Letter, the Subcontractor also secures a Direction Letter in respect of the NHSPS Eligible Employees for their future service with the Subcontractor as a condition of being awarded the Sub-Contract and the Supplier shall be responsible for ensuring that the Buyer receives a complete copy of each such Subcontractor direction letter as soon as reasonably practicable; or
 - 8.1.2 if, in accordance with Paragraph 4 of this Annex, the Supplier has offered the NHSPS Eligible Employees access to a pension scheme under which the benefits are Broadly Comparable to those provided under the NHSPS, the Subcontractor either secures a Direction Letter in respect of the NHSPS Eligible Employees or (with the prior consent of the Buyer) provides NHSPS Eligible Employees with access to a scheme with Pension Benefits which are Broadly Comparable to those provided under the NHSPS whereupon the provisions of Paragraph 10 below (Bulk Transfer Obligations in relation to any Broadly Comparable Scheme) shall apply.
- 8.2 The Supplier shall procure that each Subcontractor provides indemnities to the Buyer, NHS Pensions and/or any Replacement Supplier and/or Replacement Subcontractor that are identical to the indemnities set out in Paragraph 7 of this Annex D2. Where a Subcontractor fails to satisfy any claim made under such one or more indemnities, the Supplier will be liable for satisfying any such claim as if it had provided the indemnity itself.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Annex D3:

Local Government Pension Schemes (LGPS)

[Guidance: Note the LGPS unlike the CSPA & NHSPS is a funded scheme which has associated cost implications as follows:

There is not 1 LGPS but approx. 90 different Funds, each with their own separate Scheme Employer and Administering Authority, it is important to identify the correct one(s) and amend the definition of "Fund" accordingly.

It is important to check whether CCS and or the Buyer can actually participate in the LGPS. Where a government department is taking on services which were formerly the responsibility of a Local Authority it may be necessary to obtain secretary of state approval for participation in the LGPS, this is because the services are being provided to Gov. Dept. and not to a Local Authority.

Unlike New Fair Deal the 2007 Best Value pension direction does not provide a right to bulk transfer past service. Whilst typically before the 2007 direction LA did provide such a right, it is a significant additional cost and therefore bulk transfer wording has been excluded. If required take legal advice due to the exceptionally high costs which can result from a requirement to provide bulk transfers.]

1. Definitions

1.1 In this Annex D3: LGPS to Part D: Pensions, the following words have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Administering Authority"	relation to the Fund [insert name] , the relevant Administering Authority of that Fund for the purposes of the Local Government Pension Scheme Regulations 2013;
"Fund Actuary"	actuary to a Fund appointed by the Administering Authority of that Fund;
"Fund"	[insert name], a pension fund within the LGPS;
"LGPS"	Local Government Pension Scheme as governed by the LGPS Regulations, and any other regulations (in each case as amended from time to time) which are from time to time applicable to the Local Government Pension Scheme;
"LGPS Admission Agreement"	admission agreement within the meaning in Schedule 1 of the Local Government Pension Scheme Regulations 2013;
"LGPS Admission Body"	admission body (within the meaning of Part 3 of Schedule 2 of the Local Government Pension Scheme Regulations 2013);

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

"LGPS Eligible Employees"	Fair Deal Employee who at the relevant time is an eligible employee as defined in the LGPS Admission Agreement or otherwise any Fair Deal Employees who immediately before the Relevant Transfer Date was a member of, or was entitled to become a member of, or but for their compulsory transfer of employment would have been entitled to be or become a member of, the LGPS or of a scheme Broadly Comparable to the LGPS; and
"LGPS Regulations"	Local Government Pension Scheme Regulations 2013 (SI 2013/2356) and The Local Government Pension Scheme (Transitional Provisions, Savings and Amendment) Regulations 2014, and any other regulations(in each case as amended from time to time) which are from time to time applicable to the LGPS.

2. Supplier must become a LGPS admission body

- 2.1 Where the Supplier employs any LGPS Eligible Employees from a Relevant Transfer Date, the Supplier shall become an LGPS Admission Body and shall on or before the Relevant Transfer Date enter into a LGPS Admission Agreement with the Administering Authority which will have effect from and including the Relevant Transfer Date.
- 2.2 The LGPS Admission Agreement must ensure that all LGPS Eligible Employees covered by that Agreement who were active LGPS members immediately before the Relevant Transfer Date are admitted to the LGPS with effect on and from the Relevant Transfer Date. Any LGPS Eligible Employees who were eligible to join the LGPS but were not active LGPS members immediately before the Relevant Transfer Date must retain the ability to join the LGPS after the Relevant Transfer Date if they wish to do so.
- 2.3 The Supplier shall provide any indemnity, bond or guarantee required by an Administering Authority in relation to an LGPS Admission Agreement.
- 2.4 The Supplier shall not automatically enrol or re-enrol for the purposes of the Pensions Act 2008 any LGPS Eligible Employees in any pension scheme other than the LGPS.

3. Right of set-off

The Buyer shall have a right to set off against any payments due to the Supplier under the Contract an amount equal to any overdue employer and employee contributions and other payments (and interest payable under the LGPS Regulations) due from the Supplier (or from any relevant Subcontractor) under an LGPS Admission Agreement and shall pay such amount to the relevant Fund.

4. Supplier ceases to be an LGPS Admission Body

If the Supplier employs any LGPS Eligible Employees from a Relevant Transfer Date and the Supplier either cannot or does not participate in the LGPS, the Supplier shall offer

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

such LGPS Eligible Employee membership of a pension scheme Broadly Comparable to the LGPS.

5. Discretionary benefits

Where the Supplier is an LGPS Admission Body, the Supplier shall award benefits to the LGPS Eligible Employees under the LGPS in circumstances where the LGPS Eligible Employees would have received such benefits had they still been employed by their previous employer. Where such benefits are of a discretionary nature, they shall be awarded on the basis of the previous employer's written policy in relation to such benefits at the time of the Relevant Transfer Date.

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Annex D4: Other Schemes

[Guidance: Placeholder for Pension Schemes other than LGPS, CSPA & NHSPS]

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

Part E: Staff Transfer on Exit

1. Obligations before a Staff Transfer

1.1 The Supplier agrees that within 20 Working Days of the earliest of:

- 1.1.1 receipt of a notification from the Buyer of a Service Transfer or intended Service Transfer;
- 1.1.2 receipt of the giving of notice of early termination or any Partial Termination of the relevant Contract;
- 1.1.3 the date which is 12 Months before the end of the Term; and
- 1.1.4 receipt of a written request of the Buyer at any time (provided that the Buyer shall only be entitled to make one such request in any 6 Month period),

it shall provide in a suitably anonymised format so as to comply with the Data Protection Laws, the Supplier's Provisional Supplier Personnel List, together with the Staffing Information in relation to the Supplier's Provisional Supplier Personnel List and it shall provide an updated Supplier's Provisional Supplier Personnel List at such intervals as are reasonably requested by the Buyer.

- 1.2 At least 20 Working Days prior to the Service Transfer Date, the Supplier shall provide to the Buyer or at the direction of the Buyer to any Replacement Supplier and/or any Replacement Subcontractor (i) the Supplier's Final Supplier Personnel List, which shall identify the basis upon which they are Transferring Supplier Employees and (ii) the Staffing Information in relation to the Supplier's Final Supplier Personnel List (insofar as such information has not previously been provided).
- 1.3 The Buyer shall be permitted to use and disclose information provided by the Supplier under paragraphs 1.1 and 1.2 for the purpose of informing any prospective Replacement Supplier and/or Replacement Subcontractor.
- 1.4 The Supplier warrants, for the benefit of The Buyer, any Replacement Supplier, and any Replacement Subcontractor that all information provided pursuant to paragraphs 1.1 and 1.2 shall be true and accurate in all material respects at the time of providing the information.
- 1.5 From the date of the earliest event referred to in Paragraph 1.1.1, 1.1.2 and 1.1.3, the Supplier agrees that it shall not assign any person to the provision of the Services who is not listed on the Supplier's Provisional Supplier Personnel List and shall, unless otherwise instructed by the Buyer (acting reasonably):

not replace or re-deploy any Supplier Personnel listed on the Supplier Provisional Supplier Personnel List other than where any replacement is of equivalent grade, skills, experience and expertise and is employed on the same terms and conditions of employment as the person he/she replaces

not make, promise, propose, permit or implement any material changes to the terms and conditions of (i) employment and/or (ii) pensions, retirement and death benefits (including not to make pensionable any category of earnings which were not

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

previously pensionable or reduce the pension contributions payable) of the Supplier Personnel (including any payments connected with the termination of employment);

- 1.5.1 not increase the proportion of working time spent on the Services (or the relevant part of the Services) by any of the Supplier Personnel save for fulfilling assignments and projects previously scheduled and agreed;
- 1.5.2 not introduce any new contractual or customary practice concerning the making of any lump sum payment on the termination of employment of any employees listed on the Supplier's Provisional Supplier Personnel List;
- 1.5.3 not increase or reduce the total number of employees so engaged, or deploy any other person to perform the Services (or the relevant part of the Services);
- 1.5.4 not terminate or give notice to terminate the employment or contracts of any persons on the Supplier's Provisional Supplier Personnel List save by due disciplinary process;
- 1.5.5 not dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Buyer and/or the Replacement Supplier and/or Replacement Subcontractor;
- 1.5.6 give the Buyer and/or the Replacement Supplier and/or Replacement Subcontractor reasonable access to Supplier Personnel and/or their consultation representatives to inform them of the intended transfer and consult any measures envisaged by the Buyer, Replacement Supplier and/or Replacement Subcontractor in respect of persons expected to be Transferring Supplier Employees;
- 1.5.7 co-operate with the Buyer and the Replacement Supplier to ensure an effective consultation process and smooth transfer in respect of Transferring Supplier Employees in line with good employee relations and the effective continuity of the Services, and to allow for participation in any pension arrangements to be put in place to comply with New Fair Deal;
- 1.5.8 promptly notify the Buyer or, at the direction of the Buyer, any Replacement Supplier and any Replacement Subcontractor of any notice to terminate employment given by the Supplier or received from any persons listed on the Supplier's Provisional Supplier Personnel List regardless of when such notice takes effect;
- 1.5.9 not for a period of 12 Months from the Service Transfer Date re-employ or re-engage or entice any employees, suppliers or Subcontractors whose employment or engagement is transferred to the Buyer and/or the Replacement Supplier (unless otherwise instructed by the Buyer (acting reasonably));
- 1.5.10 not to adversely affect pension rights accrued by all and any Fair Deal Employees in the period ending on the Service Transfer Date;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 1.5.11 fully fund any Broadly Comparable pension schemes set up by the Supplier;
 - 1.5.12 maintain such documents and information as will be reasonably required to manage the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Subcontractor in the provision of the Services on the expiry or termination of this Contract (including without limitation identification of the Fair Deal Employees);
 - 1.5.13 promptly provide to the Buyer such documents and information mentioned in Paragraph 3.1.1 of Part D: Pensions which the Buyer may reasonably request in advance of the expiry or termination of this Contract; and
 - 1.5.14 fully co-operate (and procure that the trustees of any Broadly Comparable pension scheme shall fully co-operate) with the reasonable requests of the Supplier relating to any administrative tasks necessary to deal with the pension aspects of any onward transfer of any person engaged or employed by the Supplier or any Subcontractor in the provision of the Services on the expiry or termination of this Contract.
- 1.6 On or around each anniversary of the Effective Date and up to four times during the last 12 Months of the Term, the Buyer may make written requests to the Supplier for information relating to the manner in which the Services are organised. Within 20 Working Days of receipt of a written request the Supplier shall provide such information as the Buyer may reasonably require which shall include:
 - 1.6.1 the numbers of employees engaged in providing the Services;
 - 1.6.2 the percentage of time spent by each employee engaged in providing the Services;
 - 1.6.3 the extent to which each employee qualifies for membership of any of the Fair Deal Schemes (as defined in Part D: Pensions); and
 - 1.6.4 a description of the nature of the work undertaken by each employee by location.
- 1.7 The Supplier shall provide all reasonable cooperation and assistance to the Buyer, any Replacement Supplier and/or any Replacement Subcontractor to ensure the smooth transfer of the Transferring Supplier Employees on the Service Transfer Date including providing sufficient information in advance of the Service Transfer Date to ensure that all necessary payroll arrangements can be made to enable the Transferring Supplier Employees to be paid as appropriate. Without prejudice to the generality of the foregoing, within 5 Working Days following the Service Transfer Date, the Supplier shall provide to the Buyer or, at the direction of the Buyer, to any Replacement Supplier and/or any Replacement Subcontractor (as appropriate), in respect of each person on the Supplier's Final Supplier Personnel List who is a Transferring Supplier Employee:
 - 1.7.1 the most recent month's copy pay slip data;
 - 1.7.2 details of cumulative pay for tax and pension purposes;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 1.7.3 details of cumulative tax paid;
- 1.7.4 tax code;
- 1.7.5 details of any voluntary deductions from pay; and
- 1.7.6 bank/building society account details for payroll purposes.

2. Staff Transfer when the contract ends

- 2.1 A change in the identity of the supplier of the Services (or part of the Services), howsoever arising, may constitute a Relevant Transfer to which the Employment Regulations will apply. The Buyer and the Supplier agree that where a Relevant Transfer occurs, the contracts of employment between the Supplier and the Transferring Supplier Employees (except in relation to any contract terms disappplied through operation of regulation 10(2) of the Employment Regulations) will have effect on and from the Service Transfer Date as if originally made between the Replacement Supplier and/or a Replacement Subcontractor (as the case may be) and each such Transferring Supplier Employee.
- 2.2 The Supplier shall comply with all its obligations in respect of the Transferring Supplier Employees arising under the Employment Regulations in respect of the period up to (and including) the Service Transfer Date including (without limit) the payment of all remuneration, benefits, entitlements, PAYE, national insurance contributions and pension contributions and all such sums due as a result of any Fair Deal Employees' participation in the Fair Deal Schemes (as defined in Part D: Pensions).
- 2.3 Subject to Paragraph 2.4, the Supplier shall indemnify the Buyer and/or the Replacement Supplier and/or any Replacement Subcontractor against any Employee Liabilities arising from or as a result of any act or omission of the Supplier or any Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee representative (as defined in the Employment Regulations) of any Transferring Supplier Employee whether occurring before, on or after the Service Transfer Date.
- 2.4 The indemnity in paragraph 2.3 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Replacement Supplier and/or any Replacement Subcontractor whether occurring or having its origin before, on or after the Service Transfer Date.
- 2.5 Subject to Paragraphs 2.6 and 2.7, if any employee of the Supplier who is not identified in the Supplier's Final Transferring Supplier Employee List claims, or it is determined in relation to any employees of the Supplier, that his/her contract of employment has been transferred from the Supplier to the Replacement Supplier and/or Replacement Subcontractor pursuant to the Employment Regulations then.
 - 2.5.1 the Replacement Supplier and/or Replacement Subcontractor will, within 5 Working Days of becoming aware of that fact, notify the Buyer and the Supplier in writing;
 - 2.5.2 the Supplier may offer employment to such person, or take such other steps as it considered appropriate to resolve the matter, within 10 Working Days of receipt of notice from the Replacement Supplier and/or Replacement Subcontractor;

Call-Off Schedule 2 (Staff Transfer)

Call-Off Ref:

Crown Copyright 2021

- 2.5.3 if such offer of employment is accepted, the Replacement Supplier and/or Replacement Subcontractor shall immediately release the person from its employment;
 - 2.5.4 if after the period referred to in Paragraph 2.5.2 no such offer has been made, or such offer has been made but not accepted, the Replacement Supplier and/or Replacement Subcontractor may within 5 Working Days give notice to terminate the employment of such person;
 - 1. and subject to the Replacement Supplier's and/or Replacement Subcontractor's compliance with Paragraphs 2.5.1 to 2.5.4 the Supplier will indemnify the Replacement Supplier and/or Replacement Subcontractor against all Employee Liabilities arising out of the termination of the employment of any of the Supplier's employees referred to in Paragraph 2.5.
- 2.6 The indemnity in Paragraph 2.5 shall not apply to:
 - 2.6.1 (a) any claim for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief, or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees, arising as a result of any alleged act or omission of the Replacement Supplier and/or Replacement Subcontractor, or
 - 2.6.2 (b) any claim that the termination of employment was unfair because the Replacement Supplier and/or Replacement Subcontractor neglected to follow a fair dismissal procedure.
- 2.7 The indemnity in Paragraph 2.5 shall not apply to any termination of employment occurring later than 3 Months from the Service Transfer Date.
- 2.8 If at any point the Replacement Supplier and/or Replacement Subcontractor accepts the employment of any such person as is described in Paragraph 2.5, such person shall be treated as a Transferring Supplier Employee and Paragraph 2.5 shall cease to apply to such person.
- 2.9 The Supplier shall promptly provide the Buyer and any Replacement Supplier and/or Replacement Subcontractor, in writing such information as is necessary to enable the Buyer, the Replacement Supplier and/or Replacement Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations. The Buyer shall procure that the Replacement Supplier and/or Replacement Subcontractor, shall promptly provide to the Supplier and each Subcontractor in writing such information as is necessary to enable the Supplier and each Subcontractor to carry out their respective duties under regulation 13 of the Employment Regulations.
- 2.10 Subject to Paragraph 2.9, the Buyer shall procure that the Replacement Supplier indemnifies the Supplier on its own behalf and on behalf of any Replacement Subcontractor and its Subcontractors against any Employee Liabilities arising from or as a result of any act or omission, whether occurring before, on or after the Service Transfer Date, of the Replacement Supplier and/or Replacement Subcontractor in respect of any Transferring Supplier Employee or any appropriate employee

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

representative (as defined in the Employment Regulations) of any such Transferring Supplier Employee.

- 2.11 The indemnity in Paragraph 2.10 shall not apply to the extent that the Employee Liabilities arise or are attributable to an act or omission of the Supplier and/or any Sub-contractor (as applicable) whether occurring or having its origin before, on or after the Service Transfer Date, including any Employee Liabilities arising from the failure by the Supplier and/or any Subcontractor (as applicable) to comply with its obligations under the Employment Regulations, or to the extent the Employee Liabilities arise out of the termination of employment of any person who is not identified in the Supplier's Final Supplier Personnel List in accordance with Paragraph 2.5 (and subject to the limitations set out in Paragraphs 2.6 and 2.7 above).

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

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:

- 2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio
- 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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 3 (Continuous Improvement)

Call-Off Ref:
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 3 (Continuous Improvement)

Call-Off Ref:

Call-Off Schedule 4 (Call-Off Tender)

Call-Off Ref:

Crown Copyright 2021

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)

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

Annex 1 (Expenses Policy)

Not applicable

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):

"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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

"Defect"	<p>any of the following:</p> <p>a) any error, damage or defect in the manufacturing of a Deliverable; or</p> <p>b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or</p>
	<p>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</p>
	<p>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;</p>
"Emergency Maintenance"	<p>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;</p>
"ICT Environment"	<p>the Buyer System and the Supplier System;</p>
"Licensed Software"	<p>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;</p>
"Maintenance Schedule"	<p>has the meaning given to it in paragraph 8 of this Schedule;</p>

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

"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;

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

"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;
"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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 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;

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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 licensee 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:

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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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) Call-Off Ref:

Crown Copyright 2021

Call-Off Schedule 7 (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, if applicable, the Statement of Work will list 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 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 three (3) Months' notice;
 - 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, and under each Statement of Work;
 - 1.5.7 on written request from the Buyer, provide details of start and end dates of engagement of all Key Staff filling Key Roles under the Call-Off Contract and, if applicable, under each Statement of Work

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 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)

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

1. Definitions

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

"BCDR Plan"	1has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster"	3the 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"	4the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	5has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	6the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	7any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	8has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	9has 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 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 Section 1 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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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.

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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 the 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.

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

9.1 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.

Call-Off Schedule 9 (Security) – Not Used and replaced with Annex A security Schedule Development

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

Part B: Long Form Security Requirements

1. Definitions

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

“Baseline Security Requirements”

are the requirements set out in Part B, Annex 1 to this Schedule;

"Breach of Security"

means the occurrence of:

- c) **any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or**
- d) **the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such**

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

information or data, used by the Buyer and/or the Supplier in connection with this Contract,

in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d);

ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response

2. Security Requirements
plans, patches to vulnerabilities and mitigations to Breaches of Security.

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 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1

2.3.2 **REDACTED TEXT under FOIA Section 40, Personal Information**

2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
- 2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

- 3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.
- 3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the

ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

- 3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and
- 3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

- 3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;
- 3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
- 3.4.3 at all times provide a level of security which:
- a) is in accordance with the Law and this Contract;
 - b) complies with the Baseline Security Requirements;

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- c) as a minimum demonstrates Good Industry Practice;
- d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
- e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)
(<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)
- f) takes account of guidance issued by the Centre for Protection of National Infrastructure (<https://www.cpni.gov.uk>)
- g) complies with HMG Information Assurance Maturity Model and Assurance Framework
(<https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm>)
- h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
- i) addresses issues of incompatibility with the Supplier's own organisational security policies; and
- j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall imme-

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

diately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

- 3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten

(10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen

(15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of

the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

- 3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

- 4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

- 4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
- 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d), the Security Policy;
- 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- 4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures

which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of

non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d), any changes to the Security Policy; and

5.1.5 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.
- Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d).

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

- a) minimise the extent of actual or potential harm caused by any Breach of Security;
- b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
- c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

- d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
- e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
- f) as soon as reasonably practicable, provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST <http://nvd.nist.gov/cvss.cfm>); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

above timescales if the vulnerability becomes exploitable within the context of the Service;

- 9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the

Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

- 9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6

Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

- 9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12

Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

- 9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

- 9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

- 9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

- 9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

- 9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

- 9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
- 9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and
- 9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline Security Requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

(<https://www.ncsc.gov.uk/guidance/end-user-device-security>). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice

Framework Ref:

RM6263

Project Version: v1.0

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (<https://www.ncsc.gov.uk/section/products-services/ncsc-certification>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.
- 6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.
- 6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

- 7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

- 8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:
- 8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

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):

"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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

	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;
"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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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

("Registers").

2.3The 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.

2.4Each 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

3.1The 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**").

3.2The 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.

3.3The Supplier shall provide complete updates of the Exit Information on an as-requested 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).

3.4The 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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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 SOW Exit Plan provisions to 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.

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

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.

4.6A 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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 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, the provision of the Management Information or any other reports nor 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 de-installation 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

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

Service Levels or KPI, 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.

Call-Off Schedule 10 (Exit Management)

Call-Off Ref:

- 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.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

8.7The 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.

8.8The 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.

8.9The 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

9.1Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

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):

"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"	1an 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"	2a payment identified in the Implementation Plan to be made following the issue of a Satisfaction Certificate in respect of Achievement of the relevant Milestone;
Implementation Period"	3has the meaning given to it in Paragraph 7.1;

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 whole Call-Off Contract and each Statement of Work issued under it for the supply of Deliverables and as the Buyer may otherwise require;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

- 2.2.2 shall provide details on how the required Social Value commitments will be delivered through the Call-Off Contract; and
 - 2.2.3 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 also provide as required or requested reports to the Buyer concerning activities and impacts arising from Social Value including in the Implementation Plan.
- 2.6 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.
- 2.7 The Supplier shall, in relation to each SOW, incorporate within it all Implementation Plan and Testing requirements for the satisfactory completion of each Deliverable Item to be provided under that SOW.

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.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

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 their 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.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

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 a [six (6)] Month period for the Call-Off Contract and for the duration of each SOW.
- 7.2 During the Implementation Period, the incumbent supplier shall retain full responsibility for all existing services until the Call-Off Start Date or as otherwise formally agreed with the Buyer in each SOW. The Supplier's full service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.
- 7.3 In accordance with the Implementation Plan, the Supplier shall:
 - 7.3.1 work cooperatively and in partnership with the Buyer, incumbent supplier, and other Framework Supplier(s), where

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;

7.3.2 work with the incumbent supplier and Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;

7.3.3 liaise with the incumbent Supplier to enable the full completion of the Implementation Period activities; and

7.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key Milestones and dependencies.

7.4 The Implementation Plan will include detail stating:

7.4.1 how the Supplier will work with the incumbent Supplier and the Buyer Authorised Representative to capture and load up information such as asset data ; and

7.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the frequency, responsibility for and nature of communication with the Buyer and end users of the Services.

7.5 In addition, the Supplier shall:

7.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;

7.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract and each SOW;

7.5.3 produce a Implementation Plan report for each Buyer Premises to encompass programmes that will fulfil all the Buyer's obligations to landlords and other tenants:

(a) the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements of the occupiers when preparing these programmes which are subject to the Buyer's approval; and

(b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

- 7.5.4 manage and report progress against the Implementation Plan both at a Call-Off Contract level (which shall include an update on costings) and SOW level;
- 7.5.5 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;
- 7.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form and each SOW) 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
- 7.5.7 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 Call-Off Contract as part of the Further Competition Procedure; and
- (b) a detailed Implementation Plan for each SOW.

A.2 The Implementation Plan is set out below and the Milestones to be Achieved are identified below:

Milestone	Deliverable Items	Duration	Milestone Description	Buyer Responsibility	Milestone Payment	Delay Payments

Milestones will be Achieved in accordance with this Call-Off Schedule 13:

(Implementation Plan and Testing) e purposes of Paragraph 9.1.2 the Delay Period Limit shall be **[insert number of days]**.

The Supplier will provide a weekly progress report on the delivery of the products

Part B - Testing

1. Definitions

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

"Component"	4any constituent parts of the Deliverables;
"Material Test Issue"	5a Test Issue of Severity Level 1 or Severity Level 2;
"Satisfaction Certificate"	6a certificate materially in the form of the document contained in Annex 2 issued by the Buyer when a Deliverable and/or Milestone has satisfied its relevant Test Success Criteria;
"Severity Level"	7the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Issue Management Log"	8a log for the recording of Test Issues as described further in Paragraph 8.1 of this Schedule;
"Test Issue Threshold"	9in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Reports"	10 the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	11 the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 6.2 of this Schedule;
"Test Strategy"	12 a strategy for the conduct of Testing as described further in Paragraph 3.2 of this Schedule;
"Test Success Criteria"	13 in relation to a Test, the test success criteria for that Test as referred to in Paragraph 5 of this Schedule;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

"Test Witness"

14 any person appointed by the Buyer pursuant to Paragraph 9 of this Schedule; and

"Testing Procedures"

15 the applicable testing procedures and Test Success Criteria set out in this Schedule.

2. How testing should work

- 2.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, Test Specification and the Test Plan.
- 2.2 The Supplier shall not submit any Deliverable for Testing:
 - 2.2.1 unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;
 - 2.2.2 until the Buyer has issued a Satisfaction Certificate in respect of any prior, dependant Deliverable(s); and
 - 2.2.3 until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).
- 2.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.
- 2.4 Prior to the issue of a Satisfaction Certificate, the Buyer shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3. Planning for testing

- 3.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Start Date but in any case no later than twenty (20) Working Days after the Start Date.
- 3.2 The final Test Strategy shall include:
 - 3.2.1 an overview of how Testing will be conducted in relation to the Implementation Plan;
 - 3.2.2 the process to be used to capture and record Test results and the categorisation of Test Issues;
 - 3.2.3 the procedure to be followed should a Deliverable fail a Test, fail to satisfy the Test Success Criteria or where the Testing of a Deliverable produces unexpected results, including a procedure for the resolution of Test Issues;
 - 3.2.4 the procedure to be followed to sign off each Test;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 3.2.5 the process for the production and maintenance of Test Reports and a sample plan for the resolution of Test Issues;
- 3.2.6 the names and contact details of the Buyer and the Supplier's Test representatives;
- 3.2.7 a high level identification of the resources required for Testing including Buyer and/or third party involvement in the conduct of the Tests;
- 3.2.8 the technical environments required to support the Tests; and
- 3.2.9 the procedure for managing the configuration of the Test environments.

4. Preparing for Testing

- 4.1 The Supplier shall develop Test Plans and submit these for Approval as soon as practicable but in any case no later than twenty (20) Working Days prior to the start date for the relevant Testing as specified in the Implementation Plan.
- 4.2 Each Test Plan shall include as a minimum:
 - 4.2.1 the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being Tested and, for each Test, the specific Test Success Criteria to be satisfied; and
 - 4.2.2 a detailed procedure for the Tests to be carried out.
- 4.3 The Buyer shall not unreasonably withhold or delay its approval of the Test Plan provided that the Supplier shall implement any reasonable requirements of the Buyer in the Test Plan.

5. Passing Testing

- 5.1 The Test Success Criteria for all Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 4.

6. How Deliverables will be tested

- 6.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days prior to the start of the relevant Testing (as specified in the Implementation Plan).
- 6.2 Each Test Specification shall include as a minimum:
 - 6.2.1 the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Buyer and the extent to which it is equivalent to live operational data;

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 6.2.2 a plan to make the resources available for Testing;
- 6.2.3 Test scripts;
- 6.2.4 Test pre-requisites and the mechanism for measuring them;
and
- 6.2.5 expected Test results, including:
 - (a) a mechanism to be used to capture and record Test results; and
 - (b) a method to process the Test results to establish their content.

7. Performing the tests

- 7.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.
- 7.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 9.3.
- 7.3 The Supplier shall notify the Buyer at least 10 Working Days in advance of the date, time and location of the relevant Tests and the Buyer shall ensure that the Test Witnesses attend the Tests.
- 7.4 The Buyer may raise and close Test Issues during the Test witnessing process.
- 7.5 The Supplier shall provide to the Buyer in relation to each Test:
 - 7.5.1 a draft Test Report not less than 2 Working Days prior to the date on which the Test is planned to end; and
 - 7.5.2 the final Test Report within 5 Working Days of completion of Testing.
- 7.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:
 - 7.6.1 an overview of the Testing conducted;
 - 7.6.2 identification of the relevant Test Success Criteria that have/have not been satisfied together with the Supplier's explanation of why any criteria have not been met;
 - 7.6.3 the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;
 - 7.6.4 the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

each case grouped by Severity Level in accordance with Paragraph 8.1; and

- 7.6.5 the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.
- 7.7 When the Supplier has completed a Milestone, it shall submit any Deliverables relating to that Milestone for Testing.
- 7.8 Each party shall bear its own costs in respect of the Testing. However, if a Milestone is not Achieved the Buyer shall be entitled to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing of a Milestone.
- 7.9 If the Supplier successfully completes the requisite Tests, the Buyer shall issue a Satisfaction Certificate as soon as reasonably practical following such successful completion. Notwithstanding the issuing of any Satisfaction Certificate, the Supplier shall remain solely responsible for ensuring that the Deliverables are implemented in accordance with this Contract.

8. Discovering Problems

- 8.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.
- 8.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Buyer upon request.
- 8.3 The Buyer shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

9. Test witnessing

- 9.1 The Buyer may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Buyer, each of whom shall have appropriate skills to fulfil the role of a Test Witness.
- 9.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

9.3 The Test Witnesses:

- 9.3.1 shall actively review the Test documentation;
- 9.3.2 will attend and engage in the performance of the Tests on behalf of the Buyer so as to enable the Buyer to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;
- 9.3.3 shall not be involved in the execution of any Test;
- 9.3.4 shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;
- 9.3.5 may produce and deliver their own, independent reports on Testing, which may be used by the Buyer to assess whether the Tests have been Achieved;
- 9.3.6 may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

- 9.4 may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

10. Auditing the quality of the test

- 10.1 The Buyer or an agent or contractor appointed by the Buyer may perform on-going quality audits in respect of any part of the Testing (each a "**Testing Quality Audit**") subject to the provisions set out in the agreed Quality Plan.
- 10.2 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.
- 10.3 The Buyer will give the Supplier at least 5 Working Days' written notice of the Buyer's intention to undertake a Testing Quality Audit.
- 10.4 The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Buyer to enable it to carry out the Testing Quality Audit.
- 10.5 If the Testing Quality Audit gives the Buyer concern in respect of the Testing Procedures or any Test, the Buyer shall prepare a written report for the Supplier detailing its concerns and the Supplier shall, within a reasonable timeframe, respond in writing to the Buyer's report.
- 10.6 In the event of an inadequate response to the written report from the Supplier, the Buyer (acting reasonably) may withhold a Satisfaction

Certificate until the issues in the report have been addressed to the reasonable satisfaction of the Buyer.

11. Outcome of the testing

- 11.1 The Buyer will issue a Satisfaction Certificate when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.
- 11.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Buyer shall notify the Supplier and:
 - 11.2.1 the Buyer may issue a Satisfaction Certificate conditional upon the remediation of the Test Issues;
 - 11.2.2 the Buyer may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or
 - 11.2.3 where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.
- 11.3 The Buyer shall be entitled, without prejudice to any other rights and remedies that it has under this Contract, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.
- 11.4 The Buyer shall issue a Satisfaction Certificate in respect of a given Milestone as soon as is reasonably practicable following:
 - 11.4.1 the issuing by the Buyer of Satisfaction Certificates and/or conditional Satisfaction Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and
 - 11.4.2 performance by the Supplier to the reasonable satisfaction of the Buyer of any other tasks identified in the Implementation Plan as associated with that Milestone.
- 11.5 The grant of a Satisfaction Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of any Implementation Plan and Clause 4 (Pricing and payments).
- 11.6 If a Milestone is not Achieved, the Buyer shall promptly issue a report to the Supplier setting out the applicable Test Issues and any other reasons for the relevant Milestone not being Achieved.

Call-Off Schedule 13: (Implementation Plan and Testing)

Call-Off Ref:

Crown Copyright 2018

- 11.7 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Buyer shall issue a Satisfaction Certificate.
- 11.8 If there is one or more Material Test Issue(s), the Buyer shall refuse to issue a Satisfaction Certificate and, without prejudice to the Buyer's other rights and remedies, such failure shall constitute a material Default.
- 11.9 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Buyer may at its discretion (without waiving any rights in relation to the other options) choose to issue a Satisfaction Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:
 - 11.9.1 any Rectification Plan shall be agreed before the issue of a conditional Satisfaction Certificate unless the Buyer agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Buyer within 10 Working Days of receipt of the Buyer's report pursuant to Paragraph 10.5); and
 - 11.9.2 where the Buyer issues a conditional Satisfaction Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date.

12.Risk

- 12.1 The issue of a Satisfaction Certificate and/or a conditional Satisfaction Certificate shall not:
 - 12.1.1 operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Buyer's requirements for that Deliverable or Milestone; or
 - 12.1.2 affect the Buyer's right subsequently to reject all or any element of the Deliverables and/or any Milestone to which a Satisfaction Certificate relates.

Annex 1: Test Issues – Severity Levels

1. Severity 1 Error

- 1.1 This is an error that causes non-recoverable conditions, e.g. it is not possible to continue using a Component.

2. Severity 2 Error

- 2.1 This is an error for which, as reasonably determined by the Buyer, there is no practicable workaround available, and which:
 - 2.1.1 causes a Component to become unusable;
 - 2.1.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or
 - 2.1.3 has an adverse impact on any other Component(s) or any other area of the Deliverables;

3. Severity 3 Error

- 3.1 This is an error which:
 - 3.1.1 causes a Component to become unusable;
 - 3.1.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or
 - 3.1.3 has an impact on any other Component(s) or any other area of the Deliverables;but for which, as reasonably determined by the Buyer, there is a practicable workaround available;

4. Severity 4 Error

- 4.1 This is an error which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Deliverables.

5. Severity 5 Error

- 5.1 This is an error that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Deliverables.

Annex 2: Satisfaction Certificate

To: [insert name of Supplier] From: [insert name of Buyer]

[insert] Date dd/mm/yyyy]

Dear Sirs,

Satisfaction Certificate

Deliverable/Milestone(s): [insert] relevant description of the agreed Deliverables/Milestones].

We refer to the agreement ("**Call-Off Contract**") [insert] Call-Off Contract reference number and any applicable SOW reference] relating to the provision of the [insert] description of the Deliverables] between the [insert] Buyer name] ("**Buyer**") and [insert Supplier name] ("**Supplier**") dated [insert] Call-Off Start Date dd/mm/yyyy].

The definitions for any capitalised terms in this certificate are as set out in the Call-Off Contract.

[We confirm that all the Deliverables relating to [insert relevant description of Deliverables/agreed Milestones and/or reference number(s) from the Implementation Plan] have been tested successfully in accordance with the Test Plan [or that a conditional Satisfaction Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria].

[OR]

[This Satisfaction Certificate is granted on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with Clause 4 (Pricing and payments)].

Yours faithfully

[insert] Name]

[insert] Position]

acting on behalf of [insert] name of Buyer]

Call-Off Schedule 14B (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):

"Critical Service Level Failure"	has the meaning given to it in the Order Form;
"Service Level Failure"	1 means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	2 shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	3 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.
- 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 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:
- 2.4.1 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;

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

Call-Off Ref:

- 2.4.2 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.

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure the Buyer shall 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

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; and/or
- 1.2.3 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. Buyer redress for failure to provide Services at or above Service Levels

- 2.1 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 12-Month rolling period.
- 2.2 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 Table

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

Part B: Performance Monitoring

2. Performance Monitoring and Performance Review

- 2.1 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.
- 2.2 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

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

Call-Off Ref:

this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

- 2.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;
 - 2.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;
 - 2.2.3 details of any Critical Service Level Failures;
 - 2.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and
 - 2.2.5 such other details as the Buyer may reasonably require from time to time.
- 2.3 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:
- 2.3.1 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;
 - 2.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 2.3.3 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.
- 2.4 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.
- 2.5 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.

3. Satisfaction Surveys

- 3.1 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 14B (Service Levels and Balanced Scorecard)

Call-Off Ref:

SECTION 2 BALANCED SCORECARD

- 1.1 As an alternative to or in addition to Service Levels (under Section 1 above) and the Supplier's performance management obligations under the Framework Contract, the Buyer and Supplier may agree to follow the Balanced Scorecard and key performance indicators ("KPIs") for a Call-Off Contract and, if applicable, one or more of its Statements of Work.

Balanced Scorecard

KPI – Performance to Pay Process			KPI – People (Resourcing)		
<p>In accordance with an agreed performance to pay process, suppliers submit the following 'inputs':</p> <ul style="list-style-type: none"> *Accurate and complete timesheets in a timely manner; *Accurate and complete Acceptance Certificates in a timely manner; *Accurate and complete Supplier Reports in a timely manner; *Accurate and complete invoices in a timely manner 			<p>Successful recruitment and placement of key resources/ provision of facilities meets the planned deliverables and contractual obligations; the supplier pro-actively manages their resource skills/ state of facilities by identifying issues early and in a timely fashion addressing any deficits.</p>		
<p>Measurement</p> <p>All of the inputs are submitted in accordance with the performance to pay process timescales and contain accurate and complete information.</p>			<p>Measurement</p> <p>*Targets met for all resources / facilities</p>		
<p>*Inputs are later than prescribed in the performance to pay process but within 5 working days of the prescribed dates.</p>			<p>*targets met for most (50%+) resources / facilities through no fault of the Buyer;</p>		
<p>*Inputs are later than 5 working days in the prescribed performance to pay process.</p>			<p>*target missed for most resources / facilities requested through no fault of the Buyer;</p>		
<p>*Inputs are incomplete or inaccurate.</p>			<p>*Inputs contain significant errors.</p>		
<p>Source: Supplier Reports/ Invoices Owner: To be agreed</p>			<p>Source: Project Managers and Wider Buyer team's verification. Owner: To be agreed</p>		
<p>KPI – Partnering Behaviours and Added Value</p> <p>*Supplier promotes positive collaborative working relationships within and across team by acting in a transparent manner. Supplier shows commitment to Buyer goals through adding value over and above the provision of compensated skilled personnel / facilities.</p>			<p>KPI – People in Place (Delivery)</p> <p>All Supplier resources delivering services for the contracts are performing to the expected standard for the skill-set supplied and/or all facilities are to the expected standard.</p>		
<p>Measurement</p> <p>*No behavioural problems identified.</p>			<p>Measurement</p> <p>*No resources are swapped out due to deficiency in skill-set and/or no change of facilities is required.</p>		
<p>*Buyer workshops attended and positive contributions made.</p>			<p>*Minor issues noted with quality of work/ standard of facilities</p>		
<p>*Added Value recognised by the programme above provision of compensated skilled resource/ facilities</p>			<p>*Few contributions made within team.</p>		
<p>*Some minor behavioural problems.</p>			<p>*No problems identified with quality of work/ state of facility</p>		
<p>*Supplier only attends some workshops or provides minor contributions.</p>			<p>*Supplier is making positive team contributions.</p>		
<p>*Supplier adds some value above provision of compensated resource/ facilities but this is not regarded as significant.</p>			<p>*Supplier skills/ facilities meet the standards expected.</p>		
<p>*Significant behavioural problems</p>			<p>*Resource is swapped out from project due to deficiency in skill-set/ change of facility is required</p>		
<p>*Supplier contributions are rare or insignificant and shows little interest in working with other suppliers</p>			<p>*Persistent issues with quality of work/ facilities noted (maybe minor ones which have persisted from one month to another)</p>		
<p>*no added value contributions recognised by Programme.</p>			<p>*Significant issue with quality of work/ facility noted in a month.</p>		
<p>Source: Collective feedback on suppliers from both Buyer and other supplier staff. Owner: To be agreed</p>			<p>Source: Project Manager and Wider Buyer team Owner: To be agreed</p>		

- 1.2 The purpose of the Balanced Scorecard is to promote contract management activity through measurement of the Supplier's performance against KPIs. The Buyer and Supplier shall agree the content of the Scorecard before the Call-Off Contract Start Date including the Material KPIs as defined in Framework Schedule 4 (Framework Management). Targets and measures to be listed in the Scorecard (example above for guidance only) should be tailored to meet the Buyer's needs and the Supplier's competences.

- 1.3 The recommended process for using the Balanced Scorecard is as follows:

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

Call-Off Ref:

- the Buyer and Supplier agree a template Balanced Scorecard together with a performance management plan which clearly outlines the responsibilities and actions that will be taken if agreed performance levels are not achieved.
- on a pre-agreed schedule (for example, Monthly) both the Buyer and the Supplier provide a rating on the Supplier's performance
- following the initial rating, both Parties meet to review the scores and agree an overall final score for each KPI
- following agreement of final scores, the process is repeating as per the agreed schedule

2. Buyer redress for failure to provide Services at or above Service Levels

2.1 The Buyer may ask for a Rectification Plan if the Supplier:

2.1.1 fails to meet [any] **OR** [Insert Number] of the key performance indicators ("KPIs") listed within Section 2 (Balanced Scorecard) ("a Default") on at least [3] occasions within a 12-Month rolling period

2.1.2 demonstrates poor performance of a Call-Off Contract and, if applicable, any Statement of Work, evidenced through Buyer feedback to CCS that the Supplier has scored a 'red' status on any one of the [4] **KPI** targets listed on the Balanced Scorecard, on at least [2] occasions within a [Call-Off Contract duration] **or** [Statement of Work duration], or within a period of 3 Months (whichever is the earlier)

2.2 This Rectification Plan must clearly detail the improvements and associated timeframes within which the Supplier shall meet and achieve the KPI targets. 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.

3. Performance Monitoring and Performance Review

3.1 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 KPIs in the Balanced Scorecard will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

3.2 The Supplier shall provide the Buyer with performance monitoring reports ("**Performance Monitoring Reports**") in accordance with the

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

process and timescales agreed which shall contain, as a minimum, the following information in respect of the relevant KPIs just ended:

- 3.2.1 for each KPI, the actual performance achieved over the relevant period;
 - 3.2.2 a summary of all failures to achieve KPIs that occurred during that period;
 - 3.2.3 details of any failures of KPIs across the Call-Off Contract and, if applicable, each one or more SOW;
 - 3.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence; and
 - 3.2.5 such other details as the Buyer may reasonably require from time to time.
- 3.3 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:
- 3.3.1 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;
 - 3.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and
 - 3.3.3 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.
- 3.4 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.
- 3.5 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 period.

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):

"Operational Board" the board established in accordance with paragraph 4.1 of this Schedule;

"Project Manager" the manager appointed in accordance with paragraph 2.1 of this Schedule;

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

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 Managers in regards to the Contract and it will be the Supplier's Contract

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

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.

Call-Off Schedule 15 (Call-Off Contract Management)

Call-Off Ref:

- 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 – in person or virtually

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. The Supplier must provide professional resources that have NSV Security Check (SC) clearance as a minimum.

2. Definitions

“Relevant Conviction” means any conviction listed in Annex 1 to this Schedule.

3. Relevant Convictions

- 3.1.1 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.
- 3.1.2 Notwithstanding Paragraph 3.1.1 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.

Worker Engagement Status (including IR35 status)

Where the Buyer has assessed its requirement and it is for Resource, the IR35 status of the Supplier Staff in Key Roles must be detailed in this Specification and, if applicable, in each Statement of Work.



Crown
Commercial
Service

Bid Pack

Attachment 3 – Statement of Requirements

Contract Reference :P5955 Infected Blood Compensation Authority Cyber and Information Security

CONTENTS

<u>1.</u>	<u>PURPOSE</u>	<u>2</u>
<u>2.</u>	<u>BACKGROUND TO THE CONTRACTING AUTHORITY</u>	<u>2</u>
<u>3.</u>	<u>BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT</u>	<u>2</u>
<u>4.</u>	<u>DEFINITIONS</u>	<u>2</u>
<u>5.</u>	<u>SCOPE OF REQUIREMENT</u>	<u>2</u>
<u>6.</u>	<u>THE REQUIREMENT</u>	<u>2</u>
<u>7.</u>	<u>KEY MILESTONES AND DELIVERABLES</u>	<u>3</u>
<u>8.</u>	<u>MANAGEMENT INFORMATION/REPORTING</u>	<u>3</u>
<u>9.</u>	<u>VOLUMES</u>	<u>3</u>

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

10.	<u>CONTINUOUS IMPROVEMENT</u>	<u>3</u>
11.	<u>SUSTAINABILITY</u>	<u>3</u>
12.	<u>QUALITY</u>	<u>4</u>
13.	<u>PRICE</u>	<u>4</u>
14.	<u>STAFF AND CUSTOMER SERVICE</u>	<u>4</u>
15.	<u>SERVICE LEVELS AND PERFORMANCE</u>	<u>4</u>
16.	<u>SECURITY AND CONFIDENTIALITY REQUIREMENTS</u>	<u>5</u>
17.	<u>PAYMENT AND INVOICING</u>	<u>5</u>
18.	<u>CONTRACT MANAGEMENT</u>	<u>5</u>
19.	<u>LOCATION</u>	<u>5</u>

1. PURPOSE

1. The Infected Blood Compensation Authority (IBCA) require a contract in place to provision professional services for cyber and information security capabilities to increase and ensure the cyber resilience of IBCA.
2. This is an urgent requirement with a delivery required to commence in Summer 2025.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

1. IBCA has been established by the Cabinet Office (CO) to deliver the Infected Blood Compensation Scheme, providing financial compensation to eligible people in the infected blood community, in response to the Infected Blood Inquiry.
2. In 2024 the Government accepted the UK Infected Blood Inquiry's recommendation to provide financial compensation to victims of infected blood, as quickly as possible.
3. IBCA will administer the Infected Blood Compensation Scheme.
4. At the current time, IBCA is part of the CO, but in time will become an independent legal entity.
5. IBCA responds directly to and is in line with the recommendations made by the Infected Blood Inquiry. Payments from the scheme to beneficiaries will be made through a user centred service - the Infected Blood Compensation Service – that will manage claim to payment.
6. The Infected Blood Compensation Service will manage the end-to-end journey from application by a potential claimant to payment to the beneficiary. At the heart of the service will be a Case Management System (CMS) as this will play a crucial role in organising, managing, and processing compensation claims efficiently and effectively. It will be designed to streamline the entire process of handling compensation claims. It centralises case information, automates workflows, facilitates communication, ensures data security and compliance, provides reporting and analytics, and enhances the overall claimant experience.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

1. IBCA are processing highly sensitive data, engaging with people that are vulnerable. IBCA are paying out substantially large amounts of money.
2. This means that IBCA needs to ensure the safety and security of those in scope of compensation, the data that IBCA holds on them along with the systems that IBCA and the people eligible to claim are using.

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

3. Cyber and information security is a critical capability to maintain the safety of people, systems and data.

1. As IBCA scales up and opens the service, the risk of wrongful and critical deception increases and it is imperative that IBCA strengthen the position of cyber and information security resilience.

1. Therefore, IBCA wishes to procure a specialist cyber and information security provider to supply professional services that can provide a wide range of security capabilities that IBCA can draw down on as required. This will ensure we have the ability to call off and call on a supplier based on the changing

1. DEFINITIONS

Expression or Acronym	Definition
CO	Cabinet Office
SIRA	Security & Information Risk Advisors
IBCA	Infected Blood Compensation Authority
CMS	Case Management System
SC	Security Check
NCSC	National Cyber Security Controls
CAF	Cyber Assessment Framework
TOGAF	The Open Group Architecture Framework
OWASP	Open Web Application Security Project
ISO27005	Information Security Risk Management (Standard)
NHS	National Health Service
KPI/SLA	Key Performance Indicator/Service Level Agreement
BC/DR	Business Continuity Management system (standard)
ISO/IEC 27001	Information technology- security techniques- information security management systems- Requirements (standard)
RAG	Red, Amber, Green (status indication)

1. SCOPE OF REQUIREMENT

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1. The supplier will provision Cyber and Information Security Professional Services to support IBCA maintain a secure environment for the data.

1. The Supplier will be required to provide:
 1. Provide a supporting virtual chief information security function
 2. Identify and manage security risks
 3. Strengthen IBCA's position against cyber-attacks
 4. Detect, respond and mitigate the impact of security incidents during core working hours (Monday-Friday 8am-6pm), however as the service evolves there may be a requirement to increase this monitoring and response to a 24/7. This would be detailed in the subsequent SoWs, including any SLAs or KPIs associated with it.
 5. Design, monitor and respond to alerts from any vulnerability scanning software implemented by IBCA
 6. Evolve security skills, knowledge and culture.

Work packages will be developed via SoWs following the award of the contract.

1. The Supplier will be required to provide the following capabilities
 1. Security Architects, Penetration Testers,
 2. Penetration Test Delivery Leads,
 3. Security & Information Risk Advisors (SIRAs)
 4. Security Analysts

1. The Buyer (IBCA) will provide:
 1. Access to infrastructure including development environments.
 2. Access to development tools.
 3. Vulnerability scanning tools.
 4. Availability of key stakeholders/teams to facilitate the assessment and action.

1. **THE REQUIREMENT**

1. The Supplier will provision professional services to assess, and strengthen the security posture of IBCA.
2. This will be done by ensuring that IBCA have the most appropriate organisational, physical, procedural, personnel and technical controls in place to manage cyber and information security risk.
3. The Supplier will ensure that IBCA controls and processes align to and meet the National Cyber Security Controls (NCSC) Cyber Assessment Framework (CAF).
4. The supplier will be expected to provide the following security capabilities:

1. **Virtual Chief Information Security Function & Support:**

1. Support the development of cyber and information security strategy, policies, and risk management.

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

2. Develop and maintain cybersecurity policies and procedures.
3. Represent the security function in executive and board discussions.
4. Oversee and optimise the security stack.
5. Ensure alignment between cybersecurity and business objectives.

1. Security Architecture:

1. Develop security architecture that are in accordance with relevant guidelines (e.g. TOGAF, OWASP).
2. Embed a secure-by-design approach into the IBCA operational delivery teams and provide implementation support, security architecture assurance, and review of high-level and low-level designs.

1. Risk Management:

1. Provide security reviews, threat assessments and threat intelligence analysis to monitor known risks and identify new ones.
2. Develop action plans for risks identified, and provide organisational wide recommendations where applicable.
3. Risk assessments should be against NCSC and in accordance with a relevant cyber and information security framework such as ISO27005.

1. Security and Privacy Assurance:

1. Provide audit and assurance activities. Examples include GovAssure, Cyber Resilience Audits and ISO27001 audits.
2. Develop assurance documentation.
3. Undertake cyber vulnerability investigations and privacy impact assessments.
4. Provide data protection implementation support.

1. Security Capability Development:

1. Undertake ISO27001, Cyber Essentials Plus and the NHS Data Protection and Security Toolkit accreditation on behalf of IBCA. This will include the development, and implementation of policy, process and governance mechanisms.
2. Review engineering practices and ensure DevSecOps is embedded.

1. Security Exercising and Testing:

1. Plan, design, develop and facilitate cyber exercises to test the resilience of IBCA across all security controls.
2. Scope and conduct security testing, and provide remediation to vulnerabilities identified.

1. Business Continuity and Disaster Recovery (BC/DR):

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1. Establish BC/DR strategy, policy and procedure that align to ISO22301 and ISO27031.
2. Implement and test BC/DR.
3. Create BC/DR incident response plans and governance.

1. Development of Active Defensive Measures:

1. Create strategies and support the implementation and configuration of systems to enable proactive detection, prevention, and response to potential threats or attacks in real-time.

1. The Supplier must:

1. Be an assured service provider (in association with NCSC) for security architecture and risk management.
2. Be accredited in Cyber Essentials Plus and ISO 27001.
3. Provision professional resources that have NSV Security Check (SC) clearance as a minimum.

1. KEY MILESTONES AND DELIVERABLES

1. The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
1	The Supplier's staff are onboarded and delivery cadence has begun.	Within 2 weeks of the contract award
2	Requests for additional resources are dealt with, and onboarded within 4 weeks after each request.	Iterative – within 4 weeks after a request for resource once initial contract resource onboard
3	There is a monthly risk management review with senior leadership.	Monthly until end of contract
4	There is a bi-weekly risk management review at the delivery team level.	Bi-weekly until end of contract
5	There is a monthly vulnerability assessment of the IBCA estate across all security controls (where applicable).	Monthly until end of contract

1. MANAGEMENT INFORMATION/REPORTING

1. The Supplier will provide a weekly progress report on the delivery of the products including:
 1. RAG status of the delivery.

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

2. The work committed to for the week and what has/has not been completed (and for those not an explanation as to why).
3. The work is committed for the next week.
4. Risks, issues and/or dependencies.

1. **CONTINUOUS IMPROVEMENT**

1. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
2. The Supplier should present new ways of working to the Authority during monthly Contract review meetings.
3. Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.
4. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

1. **SUSTAINABILITY AND SOCIAL VALUE**

1. The Social value theme for the procure is based on the Social Value model Theme 5 MAC 7.1 and 7.2

1. **QUALITY**

1. The Supplier will be able to ensure the delivery of quality outputs in accordance with the Buyers Quality Process/Strategy as well as supporting the Buyer in enhancing and improving the process and its implementation across the services.
2. The Buyer will review the Deliverables against the Acceptance Criteria and the Performance Criteria as defined in the specific SoW Form. The Supplier must:
 1. Ensure that Deliverables and any Services provided comply with the Buyer's technical and architectural standards, patterns, testing policies and deployment/release rules. The supplier must deliver the Services in a way that enables the Authority to comply with its obligations under:
 1. the Technology Code of Practice, which is available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
 2. The National Cyber Security Controls (NCSC) and the Cyber Assessment Framework (CAF) which can be found here: <https://www.ncsc.gov.uk/collection/cyber-assessment-framework>

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1. Ensure that any Deliverables are produced in accordance with the Quality Plans to ensure they are of sufficient quality and standard to meet the Acceptance Criteria as defined in the specific SoW Form.
1. Manage and escalate risks and issues as appropriate, in accordance with the provisions of the Contract.
1. The Supplier must suggest and recommend where appropriate improvements to the Services to foster best practice .
1. The supplier will internally review the outputs for pieces of work (and provide evidence of this review) before they are released for validation and testing.
1. Feedback from the buyers team will be provided on a regular basis. This will be used as a qualitative measure of quality. The supplier will be responsible for hosting retrospectives at the end of projects or significant milestones to ensure feedback is collated, documented, discussed and acted on for both the supplier and buyer.
1. Support and remediation activity should restore the service to its previous operating state and include follow-up action to prevent future occurrences.
1. Expected behaviour
 1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
 2. The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
 3. The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
 4. The Supplier must be able to commence delivery of the Services within 20 working days after the SoW Form has been jointly signed by the Parties
 5. The Supplier must adhere to the Buyer's Code of Conduct.
 6. The Supplier must take responsibility for their work as stated in the SoW Form.
 7. The Supplier must work in a collaborative manner, including with, other third party Suppliers to the Buyer and the Buyer's staff at all organisational levels.
 8. The Supplier must be able to demonstrate proactivity in sharing knowledge and experiences with members of the team with the Buyer's staff
 9. The Supplier must be able to promote ideas and provide open suggestions as applicable, demonstrating innovative ideas and value-added initiatives as part of the contract management process

1. Training and Knowledge Transfer

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1. The Supplier will be able to add value to the Buyer for example, but not limited to, by supporting IBCA teams in learning and development opportunities, providing opportunities to share learning and transfer knowledge to the Buyer's staff, adoption of best practice, mentoring and training. This will be specifically defined in any given SoW Form
2. The Supplier will be able to share and transfer knowledge to the Buyer's staff to upskill and enhance digital maturity.
3. The Supplier will be able to provide multiple data, digital and technology skill sets and expertise to deliver the required Services.
4. The Supplier will be able to train, transfer knowledge and embed social values through the delivery of the Services to ensure the Buyer's staff are up-skilled.
5. The Supplier must provide all necessary documentation when delivering the Services as defined in any given SoW Form ensuring the Buyer's staff have the necessary knowledge transferred.
6. The format and storage of any documents created by the Supplier must comply with the Buyers Data Knowledge and Information Management (DKIM) policies.

1. **PRICE**

1. Bidders are requested to complete pricing information for all specified roles in Attachment 4. It should clearly indicate the rate for all the roles in each of the tabs. All information on how this section will be evaluated is highlighted in the named attachment.
2. Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

1. **STAFF AND CUSTOMER SERVICE**

1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
2. The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
3. The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

1. **SERVICE LEVELS AND PERFORMANCE**

1. The Authority will measure the quality of the Supplier's delivery by:

SLA	Service Area	PI/SLA description	Frequency of measurement	Target
-----	--------------	--------------------	--------------------------	--------

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

	Mobilisation	The duration between the Buyer issuing the Supplier with a Project Brief and the Supplier providing the relevant information to fully populate the SoW Form within 10 working days following issuance of the draft SoW Form to the Supplier by the Buyer.	Monthly	<p>Total number of SoW Issued by Buyer/ Total number of SoW returned fully authored within 10 working days within each month.</p> <p>Target Performance Level: >95.0% Minor KPI Failure: 85.0% - 94.9% Serious KPI Failure: 75.0% - 84.9% Severe KPI Failure: 70.0% - 74.9% KPI Service Threshold: <70.0%</p>
	erly	Number of SoW completed on time and to the relevant standard issued under the Contract	erly	<p>SoWs completed on time and to the agreed standards (as detailed within the SoW), unless agreed otherwise by the Parties.</p> <p>Target Performance Level: >95.0% Minor KPI Failure: 90.0% - 94.9% Serious KPI Failure:</p>

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

				80.0% - 89.9% Severe KPI Failure: 75.0% - 79.9% KPI Service Threshold: <75.0%
--	--	--	--	---

1. SECURITY AND CONFIDENTIALITY REQUIREMENTS

1. The Supplier shall comply with the Security clauses in this Contract, including but not limited to those contained within the Additional Terms - Security Development Schedule which can be found in Attachment A.
2. The Supplier must ensure all Supplier Staff, including any Key Sub Contractor Staff or Sub Contractor Staff are as a minimum SC checked before commencing any work under this Contract. The specific SoW Form will outline the Vetting level required for that SoW
3. The Supplier will be able to provide capabilities who have been security vetted against any of the following national security vetting levels
 1. Security Check (SC)
4. The majority of capabilities will be required to be SC, however, this will be dependent on the nature of the work and defined in the SoW Form.
5. All work must be completed within the UK, offshoring of any work will not be permitted.
6. Notwithstanding the requirements of Schedule 2.4 (Security Management), any Services provided by the Supplier must comply with:
7. UK Government's Functional Security Standard 007- <https://www.gov.uk/government/publications/government-functional-standardgovs-007-security>
8. The Government Security Classification policy
9. The National Cyber Security Centre's (NCSC) information risk management guidance - <https://www.ncsc.gov.uk>
10. GDS Government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint - <https://www.gov.uk/government/publications/technology-codeofpractice/technology-code-of-practice>
11. Guidance issued by the National Protective Security Authority - <https://www.npsa.gov.uk/>
12. Notwithstanding the provisions of Call Off Order form Buyer Standards the Supplier will be required to comply with the following:

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

13. The Supplier will be able when creating products(s) align to the UK Government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:
14. GovS 002: Project delivery standards - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1002673/1195-APS-CCS0521656700-001-Project-Deliverystandard_Web.pdf
15. The Government Functional standards where it is applicable - <https://www.gov.uk/government/publications/government-functional-standardgovs-005-digital>
16. The Buyer requires the Supplier and any Key SubContractor or SubContractor to comply with the National Cyber Security Assessment framework as defined <https://www.security.gov.uk/guidance/govassure/>
17. Data Protection
 1. The Supplier shall comply with the provisions of the Contract regarding Data Protection namely Annex 1 of the call off order form.
 2. The Supplier shall ensure any obligations on Key Sub Contractors or SubContractors as outlined in the Contract are adhered to.
 3. All data and provision of services shall be held in the UK unless agreed (in writing) otherwise by the Buyer
 4. The Parties will be required to complete the Processing of Personal Data (Annex A) as found in the SoW Form for each SoW issued under this Contract
 5. The Supplier must comply with any written instructions from the Buyer when Processing Buyer Personal Data 3
 6. The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Key Sub-contractors or Subcontractors) for the provision of the Services.
 7. Please insert any specific security requirements, vetting and/or accreditation in relation to both the Supplier's staff and their systems.
 8. Please identify any confidentiality/security restrictions regarding the content of this Statement of Requirements and/or the results/deliverables of the Contract.

1. PAYMENT AND INVOICING

1. Payment can only be made following satisfactory delivery of pre-agreed certified deliverables.
2. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

Invoices should be submitted to: **REDACTED TEXT under FOIA Section 43 (2), Commercial Information**

3.

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

4. All invoices must contain a valid PO number

1. CONTRACT MANAGEMENT

1. Each SoW Form issued under this Contract will be priced using the rates detailed within the Call-Off Schedule 5. The Supplier will assign a dedicated team including a Contract Lead at their own cost, working in conjunction with the Buyer to review upcoming demand for future SoWs, escalation of problems/issues and developing the durable relationship with the Buyer
2. The Supplier's contract lead and other relevant colleagues will be required to attend various meetings including but not limited to monthly contract review meetings, this shall be attended at the Supplier's own cost. The Supplier is to provide a monthly update on work undertaken and their associated costs and remaining budget no less than five (5) working days prior to the monthly contract review meeting.
3. The Buyer requires the Supplier to be engaged at early stages of defining business problems with IBCA to assist in providing solutions and in formulation of specific SoWs
4. Meetings shall be held between the Supplier and Buyer, however, notwithstanding the provisions of this Contract, should any performance or behavioural issues occur the impacted Party shall escalate the issue within a maximum time frame of five working days to the Buyer (IBCA Deputy Director for Data) or Supplier (Contract Lead) accordingly
5. The Supplier will be expected to present new ways of working to the Buyer during the monthly contract review meetings.
6. The Supplier is required to produce project plans to be scoped for individual projects with monitoring and weekly reports provided during development sprints.
7. The required service and outcomes will be documented in each SoW Form issued under this Contract. The Supplier must under no circumstances commence any work under this Contract unless there is a SoW Form executed.
8. The Parties will execute a SoW for each requirement under this Contract. Upon execution by the Parties, each SoW will form part of this Contract. The Parties must execute a SoW for any ad-hoc Services.
9. The rights, obligations and details agreed by the Parties and set out in each SoW Form will apply only in relation to the Services that are to be delivered under that specific SoW, and will not apply to any other SoW Forms executed or to be executed under this Contract unless otherwise agreed by the Parties
10. The Supplier must not commence work on any given SoW, until the corresponding SoW Form has been signed off by the Buyer's Authorised Representative and the Supplier's Authorised Representative
11. Multiple SoWs can operate concurrently. Once executed by the Parties, no SoW Form can be changed unless the Change Request procedure have been duly completed Attendance at Contract Review meetings shall be at the Supplier's own expense.
12. The Supplier will:

Framework Ref:
RM6263

Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1. Attend an in-person on site meeting every month to review progress against the contract deliverables.
2. Provide a weekly progress report to the Head of Cyber and Information Security, and Deputy Director of Data Operations.
3. The Supplier will:
 1. Attend an in-person on site meeting every month to review progress against the contract deliverables.
 2. Provide a weekly progress report to the Head of Cyber and Information Security, and Deputy Director of Data Operations.
4. Attendance at monthly progress meetings shall be at the Supplier's own expense.

1. LOCATION

1. Services will be provided in hybrid with on and off site working.

REDACTED TEXT under FOIA Section 40, Personal Information

1. ADDITIONAL TERMS

1. The following additional terms will apply to this Contract.
2. Security Management Developer Schedule - Annex 1
3. For the purpose of this contract the Buyer has deemed this agreement a Higher Risk agreement and all clauses set out in the Additional Terms- Security Developer Schedule applicable to higher risk agreements will apply.
4. Security Management Plan Template Developer Schedule - Annex 2

Framework Ref: RM6263

Project Version: v1.0

Model Version: v3.0

1



**Crown
Commercial
Service**

Framework Ref:
RM6263

Project Version: v1.0

4

Call-Off Schedule 18 (Background
Checks)
Call-Off Ref:

[BUYER]

and

[SUPPLIER]

ETHICAL WALLS AGREEMENT

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

Version 1.0
Crown Copyright 2021

Framework Ref:
RM6263
Project Version: v1.0

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

Version history:

Document last reviewed by GLD on 1 March 2020

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

This Agreement is dated [] 20[]

Between

(1) [INSERT NAME OF BUYER] (the "Buyer") (the [acting on behalf of the Crown] of [insert Buyer's address] ; and

(2) [NAME OF SUPPLIER] a [company]/[limited liability partnership] registered in England and Wales under registered number [insert registered number] whose registered office is at [insert Supplier's registered address] (the "Supplier").

together the "Parties" and each a "Party".

BACKGROUND

- A. The Buyer is obliged to ensure transparency, fairness, non-discrimination and equal treatment in relation to its procurement process pursuant to the Public Contracts Regulations 2015 (as amended) (the **PCR**). The purpose of this document ("Agreement") is to define the protocols to be followed to prevent, identify and remedy any conflict of interest (whether actual, potential or perceived) in the context of the Further Competition Procedure.
- B. The Buyer is conducting a Further Procurement Procedure for the supply of Digital Outcomes and Specialists 5 Deliverables under a Call-Off Contract (the "**Purpose**").
- C. The Buyer has an obligation to deal with conflicts of interest as set out in Regulation 24 (1) of the PCR. The concept of conflict of interest is wide. In the PCR it is described as covering at least *"any situation where relevant staff members have, directly or indirectly, a financial, economic or other personal interest which might be perceived to compromise their impartiality and independence in the context of the procurement procedure"* (Regulation 24(2)). *"Staff members"* refers to staff members of the Buyer or of a procurement service provider acting on behalf of the Buyer who are involved in the conduct of the procurement procedure or may influence the outcome of that procedure. *"Procurement service provider"* refers to a public or private body which offers ancillary purchasing activities on the market.

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

- D. Pursuant to Regulation 41 of the PCR, the Buyer is under an obligation to ensure that competition is not distorted by the participation of any Framework Contract supplier acting as a bidder in a further competition procedure. Accordingly, the Buyer has identified that a potential distortion of competition could arise as a consequence of a bidder wishing to submit a Tender for this Further Competition Procedure, where it has also performed services for the Buyer under existing contractual arrangements or as a subcontractor under those same arrangements.
- E. The Parties wish to enter into this Agreement to ensure that a set of management processes, barriers and disciplines are put in place to ensure that conflicts of interest do not arise, and that the Supplier does not obtain an unfair competitive advantage over Other Bidders.

IT IS AGREED:

1 DEFINITIONS AND INTERPRETATION

- 1.1 The following words and expressions shall have the following meanings in this agreement and its recitals:

"Affiliate" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;

"Agreement" means this ethical walls agreement duly executed by the Parties;

"Bid Team" means any Supplier, Affiliate, connected to the preparation of an FCP Response;

"Central Government Body" means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:

- a) Government Department;
- b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
- c) Non-Ministerial Department; or

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

d) Executive Agency.

“Conflicted Personnel” means any Supplier, Affiliate, staff or agents of the Supplier or an Affiliate who, because of the Supplier’s relationship with the Buyer under any Contract have or have had access to information which creates or may create a conflict of interest;

“Contract” means the [contract for [REDACTED] dated [REDACTED] between the [REDACTED] Buyer and the Supplier and/or an Affiliate;

“Control” means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and **“Controls”** and **“Controlled”** shall be interpreted accordingly;

“Effective Date” means the date of this Agreement as set out above;

“Further Competition Procedure” or **“FCP”** means an invitation to submit tenders issued by the Buyer as part of an FCP Process;

“FCP Process” means, with regard to the Purpose, the relevant procedure provided for in Framework Schedule 7 (Call-Off Award Procedure) of RM1043.7 Framework Contract which the Buyer has elected to use to select a contractor, together with all relevant information, correspondence and/or documents issued by the Buyer as part of that procurement exercise, all information, correspondence and/or documents issued by the bidders in response together with any resulting contract;

“FCP Response” means the tender submitted or to be submitted by the Supplier or an Affiliate [(or, where relevant, by an Other Bidder)] in response to an FCP;

“Other Affiliate” any person who is a subsidiary, subsidiary undertaking or holding company of any Other Bidder;

“Other Bidder” means any other bidder or potential bidder that is not the Supplier or any Affiliate that has or is taking part in the FCP Process;

“Parties” means the Buyer and the Supplier;

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

“Professional Advisor” means a supplier, subcontractor, advisor or consultant engaged by the Supplier under the auspices of compiling its FCP Response;

“Purpose” has the meaning given to it in recital B to this Agreement;

“Representative” refers to a person's officers, directors, employees, advisers and agents and, where the context admits, providers or potential providers of finance to the Supplier or any Affiliate in connection with the FCP Process and the representatives of such providers or potential providers of finance; and

“Third Party” means any person who is not a Party and includes Other Affiliates and Other Bidders.

- 1.2 Reference to the disclosure of information includes any communication or making available information and includes both direct and indirect disclosure.
- 1.3 Reference to the disclosure of information, or provision of access, by or to the Buyer or the Supplier includes disclosure, or provision of access, by or to the representatives of the Buyer or Representatives of the Supplier (as the case may be).
- 1.4 Reference to persons includes legal and natural persons.
- 1.5 Reference to any enactment is to that enactment as amended, supplemented, re-enacted or replaced from time to time.
- 1.6 Reference to clauses and recitals is to clauses of and recitals to this Agreement.
- 1.7 Reference to any gender includes any other.
- 1.8 Reference to writing includes email.
- 1.9 The terms “associate”, “holding company”, “subsidiary”, “subsidiary undertaking” and “wholly owned subsidiary” have the meanings attributed to them in the Companies Act 2006, except that for the purposes of section 1159(1)(a) of that Act, the words ‘holds a majority of the voting rights’ shall be changed to ‘holds 30% or more of the voting rights’, and other expressions shall be construed accordingly.
- 1.10 The words “include” and “including” are to be construed without limitation.
- 1.11 The singular includes the plural and vice versa.

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

1.12 The headings contained in this Agreement shall not affect its construction or interpretation.

2 ETHICAL WALLS

2.1 In consideration of the sum of £1 payable by the Buyer to the Supplier, receipt of which is hereby acknowledged, the Supplier:

2.1.1 shall take all appropriate steps to ensure that neither the Supplier nor its Affiliates and/or Representatives are in a position where, in the reasonable opinion of the Buyer, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier or its Affiliates or Representatives and the duties owed to the Buyer under the Contract or pursuant to an fair and transparent FCP Process;

2.1.2 acknowledges and agrees that a conflict of interest may arise in situations where the Supplier or an Affiliate intends to take part in the FCP Process and, because of the Supplier's relationship with the Buyer under any Contract, the Supplier, its Affiliates and/or Representatives have or have had access to information which could provide the Supplier and/or its Affiliates with an advantage and render unfair an otherwise genuine and fair competitive FCP Process; and

2.1.3 where there is or is likely to be a conflict of interest or the perception of a conflict of interest of any kind in relation to the FCP Process, shall comply with Clause 2.2.

2.2 The Supplier shall:

2.2.1 Not assign any of the Conflicted Personnel to the Bid Team at any time;

2.2.2 Provide to the Buyer a complete and up to date list of the Conflicted Personnel and the Bid Team and reissue such list upon any change to it;

2.2.3 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates results in information of any kind or in any format and however so stored:

(a) about the Contract, its performance, operation and all matters connected or ancillary to it becoming available to the Bid Team; and/or

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

- (b) which would or could in the opinion of the Buyer confer an unfair advantage on the Supplier in relation to its participation in the FCP Process becoming available to the Bid Team;
 - 2.2.4 Ensure that by no act or omission by itself, its staff, agents and/or Affiliates and in particular the Bid Team results in information of any kind or in any format and however so stored about the FCP Process, its operation and all matters connected or ancillary to it becoming available to the Conflicted Personnel;
 - 2.2.5 Ensure that confidentiality agreements which flow down the Supplier's obligations in this Agreement are entered into as necessary between the Buyer and the Supplier, its Affiliates, its staff, agents, any Conflicted Personnel, and between any other parties necessary in a form to be prescribed by the Buyer;
 - 2.2.6 physically separate the Conflicted Personnel and the Bid Team, either in separate buildings or in areas with restricted access;
 - 2.2.7 provide regular training to its staff, agents and its Affiliates to ensure it is complying with this Agreement;
 - 2.2.8 monitor Conflicted Personnel movements within restricted areas (both physical and electronic online areas) to ensure it is complying with this Agreement ensure adherence to the ethical wall arrangements;
 - 2.2.9 ensure that the Conflicted Personnel and the Bid Team are line managed and report independently of each other; and
 - 2.2.10 comply with any other action as the Buyer, acting reasonably, may direct.
- 2.3 In addition to the obligations set out in Clause 2.1.1 and 2.1.3, the Supplier shall:
- 2.3.1 notify the Buyer immediately of all perceived, potential and/or actual conflicts of interest that arise;
 - 2.3.2 submit in writing to the Buyer full details of the nature of the conflict including (without limitation) full details of the risk assessments undertaken, the impact or potential impact of the conflict, the measures and arrangements that have

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

been established and/or are due to be established to eliminate the conflict and the Supplier's plans to prevent future conflicts of interests from arising; and

2.3.3 seek the Buyer's approval thereto,

which the Buyer shall have the right to grant, grant conditionally or deny (if the Buyer denies its approval the Supplier shall repeat the process set out in clause 2.3 until such time as the Buyer grants approval or the Supplier withdraws from the FCP Process).

2.4 Any breach of Clause 2.1, Clause 2.2 or Clause 2.3 shall entitle the Buyer to exclude the Supplier or any Affiliate or Representative from the FCP Process, and the Buyer may, in addition to the right to exclude, take such other steps as it deems necessary where, in the reasonable opinion of the Buyer there has been a breach of Clause 2.1, Clause 2.2 or Clause 2.3.

2.5 The Supplier will provide, on demand, any and all information in relation to its adherence with its obligations set out under Clauses 2.1 and 2.2 as reasonably requested by the Buyer.

2.6 The Buyer reserves the right to require the Supplier to demonstrate the measures put in place by the Supplier under Clauses 2.1.3 and 2.2.

2.7 The Supplier acknowledges that any provision of information or demonstration of measures, in accordance with Clauses 2.5 and 2.6, does not constitute acceptance by the Buyer of the adequacy of such measures and does not discharge the Supplier of its obligations or liability under this Agreement.

2.8 The actions of the Buyer pursuant to Clause 2.4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Buyer.

2.9 In no event shall the Buyer be liable for any bid costs incurred by:

2.9.1 the Supplier or any Affiliate or Representative; or

2.9.2 any Other Bidder, Other Affiliate or Other Representative,

as a result of any breach by the Supplier, Affiliate or Representative of this Agreement, including, without limitation, where the Supplier or any Affiliate or Representative, or

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

any Other Bidder, Other Affiliate or Other Representative are excluded from the FCP Process.

2.10 The Supplier acknowledges and agrees that:

2.10.1 neither damages nor specific performance are adequate remedies in the event of its breach of the obligations in Clause 2; and

2.10.2 in the event of such breach by the Supplier of any of its obligations in Clause 2 which cannot be effectively remedied the Buyer shall have the right to terminate this Agreement and the Supplier's participation in the FCP Process.

3 SOLE RESPONSIBILITY

3.1 It is the sole responsibility of the Supplier to comply with the terms of this Agreement. No approval by the Buyer of any procedures, agreements or arrangements provided by the Supplier or any Affiliate or Representative to the Buyer shall discharge the Supplier's obligations.

4 WAIVER AND INVALIDITY

4.1 No failure or delay by any Party in exercising any right, power or privilege under this Agreement or by law shall constitute a waiver of that or any other right, power or privilege, nor shall it restrict the further exercise of that or any other right, power or privilege. No single or partial exercise of such right, power or privilege shall prevent or restrict the further exercise of that or any other right, power or privilege.

4.2 If any provision of this Agreement is prohibited or unenforceable in any jurisdiction in relation to any Party, such prohibition or unenforceability will not invalidate the remaining provisions of this Agreement or affect the validity or enforceability of the provisions of this Agreement in relation to any other Party or any other jurisdiction.

5 ASSIGNMENT AND NOVATION

5.1 Subject to Clause 5.2 the Parties shall not assign, novate or otherwise dispose of or create any trust in relation to any or all of its rights, obligations or liabilities under this Agreement without the prior written consent of the Buyer.

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

- 5.2 The Buyer may assign, novate or otherwise dispose of any or all of its rights, obligations and liabilities under this Agreement and/or any associated licences to:
- 5.2.1 any Central Government Body; or
 - 5.2.2 to a body other than a Central Government Body (including any private sector body) which performs any of the functions that previously had been performed by the Authority; and
 - 5.2.3 the Supplier shall, at the Buyer's request, enter into a novation agreement in such form as the Buyer reasonably specify in order to enable the Buyer to exercise its rights pursuant to this Clause 5.
- 5.3 A change in the legal status of the Buyer such that it ceases to be a Central Government Body shall not affect the validity of this Agreement and this Agreement shall be binding on any successor body to the Buyer.

6 CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

- 6.1 A person who is not a Party to this Agreement has no right under the Contract (Rights of Third Parties) Act 1999 (as amended, updated or replaced from time to time) to enforce any term of this Agreement but this does not affect any right remedy of any person which exists or is available otherwise than pursuant to that Act.

7 TRANSPARENCY

- 7.1 The Parties acknowledge and agree that the Buyer is under a legal duty pursuant to the PCR to run transparent and fair procurement processes. Accordingly, the Buyer may disclose the contents of this Agreement to potential bidders in the FCP Process, for the purposes of transparency and in order to evidence that a fair procurement process has been followed.

8 NOTICES

- 8.1 Any notices sent under this Agreement must be in writing.
- 8.2 The following table sets out the method by which notices may be served under this Agreement and the respective deemed time and proof of service:

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

Manner of Delivery	Deemed time of service	Proof of service
Email	9.00am on the first Working Day after sending	Dispatched as a pdf attachment to an email to the correct email address without any error message.
Personal delivery	On delivery, provided delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the next Working Day.	Properly addressed and delivered as evidenced by signature of a delivery receipt.
Prepaid, Royal Mail Signed For™ 1 st Class or other prepaid, next working day service providing proof of delivery.	At the time recorded by the delivery service, provided that delivery is between 9.00am and 5.00pm on a Working Day. Otherwise, delivery will occur at 9.00am on the same Working Day (if delivery before 9.00am) or on the next Working Day (if after 5.00pm).	Properly addressed prepaid and delivered as evidenced by signature of a delivery receipt.

8.3 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Agreement:

	Supplier	Buyer
Contact	REDACTED TEXT under FOIA Section 40, Personal Information	REDACTED TEXT under FOIA Section 40, Personal Information

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:
Address

Call-Off Schedule 18 (Background Checks)

Call-Off Ref:

Email	REDACTED TEXT under FOIA Section 40, Personal Information
-------	---

- 8.4 This Clause 8 does not apply to the service of any proceedings or other documents in any legal action or other method of dispute resolution.

9 WAIVER AND CUMULATIVE REMEDIES

- 9.1 The rights and remedies under this Agreement may be waived only by notice and in a manner that expressly states that a waiver is intended and what is waived. A failure or delay by a Party in ascertaining or exercising a right or remedy provided under this Agreement or by law shall not constitute a waiver of that right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.
- 9.2 Unless otherwise provided in this Agreement, rights and remedies under this Agreement are cumulative and do not exclude any rights or remedies provided by law, in equity or otherwise.

10 TERM

- 10.1 Each Party's obligations under this Agreement shall continue in full force and effect for a period of [] years from the Effective Date.

11 GOVERNING LAW AND JURISDICTION

- 11.1 This Agreement and any issues, disputes or claims (whether contractual or non-contractual) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of England and Wales.
- 11.2 The Parties agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Agreement or its subject matter or formation.

Signed by the Buyer

Name:

Joint Schedule 2 (Variation Form)

Signature: Position in

Buyer:

Signed by the Supplier

Name: Signature:

Position in Supplier:

Joint Schedule 1 (Definitions)

- 1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.
- 1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.
- 1.3 In each Contract, unless the context otherwise requires:
 - 1.3.1 the singular includes the plural and vice versa;
 - 1.3.2 reference to a gender includes the other gender and the neuter;
 - 1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Central Government Body;
 - 1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;
 - 1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";
 - 1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;
 - 1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings**" as references to obligations under the Contract;
 - 1.3.8 references to "**Clauses**" and "**Schedules**" are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;
 - 1.3.9 references to "**Paragraphs**" are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;
 - 1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;
 - 1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract;
 - 1.3.12 where the Buyer is a Central Government Body it shall be treated as contracting with the Crown as a whole;

Joint Schedule 2 (Variation Form)

1.3.13 where a standard, policy or document is referred to by reference of a hyperlink, if that hyperlink is changed or no longer provides access to the relevant standard, policy or document, the Supplier shall notify the Relevant Authority and the Parties shall update the reference to a replacement hyperlink;

1.3.14 any reference in a Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

- (a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 shall be read on and after Exit Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
- (b) any EU institution or EU authority or other such EU body shall be read on and after Exit Day as a reference to the UK institution, authority or body to which its functions were transferred; and

1.3.15 unless otherwise provided, references to "**Buyer**" shall be construed as including Exempt Buyers; and

1.3.16 unless otherwise provided, references to "**Call-Off Contract**" and "**Contract**" shall be construed as including Exempt Call-off Contracts.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

" Achieve "	in respect of a Test, to successfully pass such Test without any Test Issues and in respect of a Milestone, the issue of a Satisfaction Certificate in respect of that Milestone if specified within the Buyer's acceptance testing procedure and " Achieved ", " Achieving " and " Achievement " shall be construed accordingly;
" Additional insurances "	insurance requirements relating to a Call-Off Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements);
" Admin Fee "	means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees ;
" Affected Party "	the Party seeking to claim relief in respect of a Force Majeure Event;
" Affiliates "	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
" Annex "	extra information which supports a Schedule;
" Approval "	the prior written consent of the Buyer and " Approve " and " Approved " shall be construed accordingly;

Joint Schedule 2 (Variation Form)

"Audit"	<p>the Relevant Authority's right to:</p> <ul style="list-style-type: none"> a) verify the accuracy of the Charges and any other amounts payable by a Buyer under a Call-Off Contract (including proposed or actual variations to them in accordance with the Contract); b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services; c) verify the Open Book Data; d) verify the Supplier's and each Subcontractor's compliance with the Contract and applicable Law; e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations; f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables; g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract; i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts; j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources; or k) verify the accuracy and completeness of any Management Information delivered or required by the Framework Contract;
"Auditor"	<ul style="list-style-type: none"> a) the Relevant Authority's internal and external auditors; b) the Relevant Authority's statutory or regulatory auditors; c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office; d) HM Treasury or the Cabinet Office;
	<ul style="list-style-type: none"> e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and f) successors or assigns of any of the above;

Joint Schedule 2 (Variation Form)

"Authority"	CCS and each Buyer;
"Authority Cause"	any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier;
"Authorised User"	CCS' and Buyers' individual or group of individuals (including employees, consultants, contractors and agents) authorised by CCS and/or the Buyer to: a) access and use the Platform for the purposes set out in Framework Schedule 7 (Call-Off Award Procedure); and b) the rights granted under (a) shall apply unless and until that authorisation is revoked by CCS or the Buyer;
"BACS"	the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom;
"Balanced Scorecard"	a tool for Call-Off Contract management activity, through measurement of a Supplier's performance against key performance indicator, which the Buyer and Supplier may agree at the Call-Off Contract Start Date;
"Beneficiary"	a Party having (or claiming to have) the benefit of an indemnity under this Contract;
"Buyer"	the relevant public sector purchaser identified as such in the Order Form;
"Buyer Assets"	the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract;
"Buyer Authorised Representative"	the representative appointed by the Buyer from time to time in relation to the Call-Off Contract initially identified in the Order Form;
"Buyer Premises"	premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them);
"Buyer Registration Process"	the process to be completed in accordance with Framework Schedule 7 (Call-Off Award Procedure) or as otherwise notified to the Buyer in writing by CCS, the completion of which shall result in a potential Buyer being registered as a "Buyer" within the Platform which will entitle the Buyer to undertake a Call-Off Procedure in accordance with Framework Schedule 7, as supported by the Platform;

Joint Schedule 2 (Variation Form)

"Buyer's Guidance"	guidance for Buyers on how to buy digital services using the Framework Contract, located at the CCS website: https://www.crowncommercial.gov.uk/agreements/RM6263 ;
"Call-Off Contract"	the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the Framework Contract), which consists of the terms set out and referred to in the Order Form;
"Call-Off Contract Period"	the Contract Period in respect of the Call-Off Contract;
"Call-Off Expiry Date"	the latter of: a) the scheduled date of the end of a Call-Off Contract as stated in the Order Form; or b) the date of completion of the last Deliverable due under the last Statement of Work under the Call-Off Contract;
"Call-Off incorporated Terms"	the contractual terms applicable to the Call-Off Contract specified under the relevant heading in the Order Form;
"Call-Off Initial Period"	the Initial Period of a Call-Off Contract specified in the Order Form;
"Call-Off Optional Extension Period"	such period or periods beyond which the Call-Off Initial Period may be extended as specified in the Order Form;
"Call-Off Procedure"	the process for awarding a Call-Off Contract pursuant to Clause 2 (How the contract works) and Framework Schedule 7 (Call-Off Award Procedure);
"Call-Off Special Terms"	any additional terms and conditions specified in the Order Form incorporated into the applicable Call-Off Contract;
"Call-Off Start Date"	the date of start of a Call-Off Contract as stated in the Order Form;
"Call-Off Tender"	the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following a Further Competition Procedure and set out at Call-Off Schedule 4 (Call-Off Tender);
"Cap"	the maximum amount to be paid by the Buyer under a Time and Materials mechanism for the delivery of an agreed scope;
"Capped Time and Materials"	Time and Materials payable up to a specified Cap for delivery of the agreed scope of Deliverables;
"CaM Tool"	the capability assessment matrix (CAM) is a downselect or multiidentifier functionality tool within the Platform to be used by Buyers to identify capable suppliers able to meet its Statement of Requirements by means of (a) ranking the suppliers, or (b) shortlisting the suppliers, which is comprised of Resource Profile, Service Capability, Location and Scalability as described in and a copy of the CaM Tool is in Annex C of Framework Schedule 7 (Call-Off Award Procedure);

Joint Schedule 2 (Variation Form)

"CCS"	the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP;
"CCS Authorised Representative"	the representative appointed by CCS from time to time in relation to the Framework Contract initially identified in the Framework Award Form;
"Central Government Body"	<p>a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none"> a) Government Department; b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); c) Non-Ministerial Department; or d) Executive Agency;
"Change in Law"	any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date;
"Change of Control"	<p>is:</p> <ul style="list-style-type: none"> a) a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; or b) any instance where the Supplier demerges into 2 or more firms, merges with another firm, incorporated or otherwise changes its legal form;
"Charges"	the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Call-Off Contract, as set out in the Order Form and, if applicable, each Statement of Work, for the full and proper performance by the Supplier of its obligations under the Call-Off Contract less any Deductions;
"Claim"	any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract;
"Commercially Sensitive Information"	the Confidential Information listed in the Framework Award Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss;
"Comparable Supply"	the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;

Joint Schedule 2 (Variation Form)

"Confidential Information"	any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS, as the context requires;
"Contract"	either the Framework Contract or the Call-Off Contract, as the context requires;
"Contract Period"	the term of either a Framework Contract or Call-Off Contract on and from the earlier of the: applicable Start Date; or the Effective Date, up to and including the applicable End Date;
"Contract Value"	the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier;
"Contract Year"	a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof;
"Control"	<ul style="list-style-type: none"> a) control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010; or b) any instance where the Supplier demerges into 2 or more firms, merges with another firm, incorporated or otherwise changes its legal form; and "Controlled" shall be construed accordingly;
"Controller"	has the meaning given to it in the UK GDPR;
"Core Terms"	CCS' terms and conditions for common goods and services which govern how Suppliers must interact with CCS and Buyers under Framework Contracts and Call-Off Contracts;

**Joint Schedule 2 (Variation
Form)**

"Costs"	<p>the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:</p> <p>a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Work Day, of engaging the Supplier Staff, including:</p> <p>i) base salary paid to the Supplier Staff; ii) employer's National Insurance contributions; iii) pension contributions;</p>
----------------	--

Joint Schedule 2 (Variation Form)

	<p>iv) car allowances;</p> <p>v) any other contractual employment benefits;</p> <p>vi) staff training; vii) work place accommodation; viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and</p> <p>ix) reasonable recruitment costs, as agreed with the Buyer;</p> <p>b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;</p> <p>c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables; and</p> <p>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables; but</p> <p>excluding:</p> <p>Overhead;</p> <p>financing or similar costs; iii) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Call-Off Contract Period whether in relation to Supplier Assets or otherwise;</p> <p>taxation;</p> <p>finances and penalties; vi) amounts payable under Call-Off Schedule 16 (Benchmarking) where such Schedule is used; and</p> <p>vii) non-cash items (including depreciation, amortisation, impairments and movements in provisions);</p>
"CRTPA"	the Contract Rights of Third Parties Act 1999;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;

Joint Schedule 2 (Variation Form)

"Data Protection Legislation"	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy;
"Data Protection Liability Cap"	the amount specified in the Framework Award Form;
"Data Protection Officer"	has the meaning given to it in the UK GDPR;
"Data Subject"	has the meaning given to it in the UK GDPR;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
"Day Rate"	the Pricing Mechanism where the Supplier will invoice the Buyer for Supplier Staff providing Deliverables (or one or more of the elements of the Deliverables) based on a rate for no more than 7.5 Work Hours performed by the Supplier's Staff based on the applicable grade(s) set out in Annex 1 of Framework Schedule 3 (Framework Prices);
"Deductions"	all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under a Call-Off Contract;
"Default"	any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority;
"Default Management Charge"	has the meaning given to it in Paragraph 8.1.1 of Framework Schedule 5 (Management Charges and Information);
"Delay Payments"	the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan;
"Deliverables"	Goods and/or Services that may be ordered under the Contract including the Documentation;
"Delivery"	delivery of the relevant Deliverable or Milestone in accordance with the terms of a Call-Off Contract as confirmed and accepted by the Buyer by the either (a) confirmation in writing to the Supplier; or (b) where Call-Off Schedule 13 (Implementation Plan and Testing) is used issue by the Buyer of a Satisfaction Certificate. "Deliver" and "Delivered" shall be construed accordingly;
"Disclosing Party"	the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential);

Joint Schedule 2 (Variation Form)

"Dispute"	any claim, dispute or difference (whether contractual or noncontractual) arising out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in Clause 34 (Resolving disputes);
"Documentation"	<p>descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:</p> <p>a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables</p> <p>b) is required by the Supplier in order to provide the Deliverables; and/or</p> <p>c) has been or shall be generated for the purpose of providing the Deliverables;</p>
"DOTAS"	the Disclosure of Tax Avoidance Schemes rules which require a promoter of Tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions;
"DPA 2018"	the Data Protection Act 2018;
"Due Diligence Information"	any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date;
"Effective Date"	the date on which the final Party has signed the Contract;
"EIR"	the Environmental Information Regulations 2004;
"Electronic Invoice"	an invoice which has been issued, transmitted and received in a structured electronic format which allows for its automatic and electronic processing and which complies with (a) the European standard and (b) any of the syntaxes published in Commission Implementing Decision (EU) 2017/1870;
"Employment Regulations"	the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC;

Joint Schedule 2 (Variation Form)

"End Date"	<p>the earlier of:</p> <p>a) the Expiry Date (as extended by any Extension Period exercised by the Relevant Authority under Clause 10.1.2); or</p> <p>b) if a Contract or Statement of Work is terminated before the date specified in (a) above, the date of termination of the Contract or Statement of Work (as the context dictates);</p>
"Environmental Policy"	<p>to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer;</p>
"Equality and Human Rights Commission"	<p>the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;</p>
"Estimated Year 1 Charges"	<p>the anticipated total Charges payable by the Buyer in the first Contract Year specified in the Order Form;</p>

"Estimated Yearly Charges"	<p>for the purposes of calculating each Party's annual liability under Clause 11.2:</p> <p>a) in the first Contract Year, the Estimated Year 1 Charges; or</p> <p>b) in the any subsequent Contract Years, the Charges paid or payable in the previous Call-off Contract Year; or</p> <p>c) after the end of the Call-off Contract, the Charges paid or payable in the last Contract Year during the Call-off Contract Period;</p>
"Exempt Buyer"	<p>a public sector purchaser that is:</p> <p>a) eligible to use the Framework Contract; and</p> <p>b) is entering into an Exempt Call-off Contract that is not subject to (as applicable) any of:</p> <p>i) the Regulations; ii) the Concession Contracts Regulations 2016 (SI 2016/273); iii) the Utilities Contracts Regulations 2016 (SI 2016/274); iv) the Defence and Security Public Contracts Regulations 2011 (SI 2011/1848);</p> <p>v) the Remedies Directive (2007/66/EC); vi) Directive 2014/23/EU of the European Parliament and Council; vii) Directive 2014/24/EU of the European Parliament and Council; viii) Directive 2014/25/EU of the European Parliament and Council; or</p>
	<p>ix) Directive 2009/81/EC of the European Parliament and Council;</p>

Joint Schedule 2 (Variation Form)

"Exempt Call-off Contract"	the contract between the Exempt Buyer and the Supplier for Deliverables which consists of the terms set out and referred to in the Order Form incorporating and, where necessary, amending, refining or adding to the terms of the Framework Contract;
"Exempt Procurement Amendments"	any amendments, refinements or additions to any of the terms of the Framework Contract made through the Exempt Call-off Contract to reflect the specific needs of an Exempt Buyer to the extent permitted by and in accordance with any legal requirements applicable to that Exempt Buyer;
"Expenses Policy"	the Buyer's expenses policy as set out in Annex 1 to Call-Off Schedule 5 (Pricing Details and Expenses Policy);

"Existing IPR"	any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise) and shall include, in the case of CCS, the website domain names www.crowncommercial.gov.uk and [Insert] regarding the Platform;
"Exit Day"	shall have the meaning in the European Union (Withdrawal) Act 2018;
"Expiry Date"	the Framework Expiry Date or the Call-Off Expiry Date (as the context dictates);
"Extension Period"	the Framework Optional Extension Period or the Call-Off Optional Extension Period as the context dictates;
"Fixed Price"	the Pricing Mechanism where Charges are agreed at a set amount in relation to all work to be done under a Contract, Statement of Work, Deliverable(s) (or one or more element of the Deliverable(s)) including all materials and/or Milestones, no matter how much work is required to complete each Contract, Statement of Work, Deliverable(s) (or one or more element of the Deliverable(s)) within the agreed scope, and the total amount to be paid by the Buyer will not exceed the agreed fixed price;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event outside the reasonable control of either Party affecting its performance of its obligations under the Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including: a) riots, civil commotion, war or armed conflict;

Joint Schedule 2 (Variation Form)

	<p>b) acts of terrorism;</p> <p>c) acts of government, local government or regulatory bodies;</p> <p>d) fire, flood, storm or earthquake or other natural disaster,</p> <p>but excluding any industrial dispute relating to the Supplier, the Supplier Staff or any other failure in the Supplier or the Subcontractor's supply chain;</p>
"Force Majeure Notice"	a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event;
"Framework Award Form"	the document outlining the Framework Incorporated Terms and crucial information required for the Framework Contract, to be executed by the Supplier and CCS;
"Framework Contract"	the framework agreement established between CCS and the Supplier in accordance with Regulation 33 by the Framework Award Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the notice published on the Find a Tender Service;
ramework Contract Period"	the period from the Framework Start Date until the End Date of the Framework Contract;
"Framework Expiry Date"	the scheduled date of the end of the Framework Contract as stated in the Framework Award Form;
"Framework Incorporated Terms"	the contractual terms applicable to the Framework Contract specified in the Framework Award Form;
"Framework Optional Extension Period"	such period or periods beyond which the Framework Contract Period may be extended as specified in the Framework Award Form;
"Framework Price(s)"	the price(s) applicable to the provision of the Deliverables set out in Framework Schedule 3 (Framework Prices);
"Framework Special Terms"	any additional terms and conditions specified in the Framework Award Form incorporated into the Framework Contract;
"Framework Start Date"	the date of start of the Framework Contract as stated in the Framework Award Form;
"Framework Tender Response"	the tender submitted by the Supplier to CCS and annexed to or referred to in Framework Schedule 2 (Framework Tender);
"Further Competition Procedure"	the further competition procedure described in Framework Schedule 7 (Call-Off Award Procedure);
"General Anti-Abuse Rule"	<p>a) the legislation in Part 5 of the Finance Act 2013 and; and</p> <p>b) any future legislation introduced into parliament to counteract Tax advantages arising from abusive arrangements to avoid National Insurance contributions;</p>

"F

Joint Schedule 2 (Variation Form)

"General Change in Law"	a Change in Law where the change is of a general legislative nature (including Tax or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply;
"Goods"	goods made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Government Data"	the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which: <ul style="list-style-type: none"> a) are supplied to the Supplier by or on behalf of the Authority; b) the Supplier is required to generate, process, store or transmit pursuant to a Contract; c) any Personal Data for which CCS or the Buyer is the Controller; or d) all Buyer Registration Process data submitted by Buyers into the Platform, including the full auditable history of any and all transactions and procedures conducted via the Platform;
"Group of Economic Operators"	a group of economic operators acting jointly and severally to provide the Deliverables, which shall include a consortium;
"Guarantor"	the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract;
"Halifax Abuse Principle"	the principle explained in the CJEU Case C-255/02 Halifax and others;
"HMRC"	Her Majesty's Revenue and Customs;

Joint Schedule 2 (Variation Form)

"Hourly Rate"	the Pricing Mechanism where the Supplier will invoice the Buyer for the work undertaken by Supplier Staff providing the Deliverables (or one or more of the elements of the Deliverables) under the Contract (and, if applicable, each SOW) based on the division of the applicable Supplier Staff Day Rate by no less than 7.5 being the applicable Work Day where the Supplier's Staff's the applicable Supplier Staff grade is set out in Annex 1 of Framework Schedule 3 (Framework Prices);
"ICT Policy"	the Buyer's policy and any Platform policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure;
"Impact Assessment"	<p>an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:</p> <ul style="list-style-type: none"> a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract; b) details of the cost of implementing the proposed Variation; c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the Framework Prices/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party; d) a timetable for the implementation, together with any proposals for the testing of the Variation; and e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request;
"Implementation Plan"	the plan for provision of the Deliverables set out in Call-Off Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer;
"Incremental Fixed Price"	<p>the Price Mechanism where the overall Statement of Work is based on Capped Time and Materials, but where the prices for individual Deliverables Increments are fixed prior to the work being undertaken.</p> <p>The Charges for the first Deliverable Increment or Deliverables Increments for the Statement of Work will be fixed, but the Charges for subsequent Deliverables Increments will be reviewed and refined prior to the execution of each subsequent Deliverables Increment within the same Statement of Work;</p>
"Indemnifier"	a Party from whom an indemnity is sought under this Contract;
"Independent Control"	<p>where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of Processing but does so separately from the Controller providing it with Personal Data and</p> <p>"Independent Controller" shall be construed accordingly;</p>

Joint Schedule 2 (Variation Form)

"Indexation"	the adjustment of an amount or sum in accordance with Framework Schedule 3 (Framework Prices) and the relevant Order Form;
"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
Initial Period"	the initial term of a Contract specified in the Framework Award Form or the Order Form, as the context requires;

Joint Schedule 2 (Variation Form)

Insolvency Event"	<p>with respect to any person, means:</p> <p>(a) that person suspends, or threatens to suspend, payment of its debts, or is unable to pay its debts as they fall due or admits inability to pay its debts, or:</p> <p>(i) (being a company or a LLP) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or</p> <p>(ii) (being a partnership) is deemed unable to pay its debts within the meaning of section 222 of the Insolvency Act 1986;</p> <p>) that person commences negotiations with one or more of its creditors (using a voluntary arrangement, scheme of arrangement or otherwise) with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with one or more of its creditors or takes any step to obtain a moratorium pursuant to Section 1A and Schedule A1 of the Insolvency Act 1986 other than (in the case of a company, a LLP or a partnership) for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>) another person becomes entitled to appoint a receiver over the assets of that person or a receiver is appointed over the assets of that person;</p> <p>) a creditor or encumbrancer of that person attaches or takes possession of, or a distress, execution or other such process is levied or enforced on or sued against, the whole or any part of that person's assets and such attachment or process is not discharged within 14 days;</p> <p>) that person suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business;</p> <p>) where that person is a company, a LLP or a partnership:</p> <p>(i) a petition is presented (which is not dismissed within 14 days of its service), a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that person other than for the sole purpose of a scheme for a solvent amalgamation of that person with one or more other companies or the solvent reconstruction of that person;</p> <p>(ii) an application is made to court, or an order is made, for the appointment of an administrator, or if a notice of intention to appoint an administrator is filed at Court or given or if an administrator is appointed, over that person;</p> <p>(iii) (being a company or a LLP) the holder of a qualifying floating charge over the assets of that person has become entitled to appoint or has appointed an administrative receiver; or</p>
--------------------------	---

Joint Schedule 2 (Variation Form)

	<p>(iv) (being a partnership) the holder of an agricultural floating charge over the assets of that person has become entitled to appoint or has appointed an agricultural receiver; or</p> <p>(g) any event occurs, or proceeding is taken, with respect to that person in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned above;</p>
"Installation Works"	all works which the Supplier is to carry out at any time during the CallOff Contract Period to install the Goods in accordance with the Call-Off Contract and, if applicable, each SOW;
"Intellectual Property Rights" or "IPR"	<p>a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;</p> <p>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and</p> <p>c) all other rights having equivalent or similar effect in any country or jurisdiction and the right to sue for passing off;</p>
"Invoicing Address"	the address to which the Supplier shall invoice the Buyer as specified in the Order Form;
"IPR Claim"	any action, suit, claim, demand, Loss or other liability which the Relevant Authority or Central Government Body may suffer or incur as a result of any claim that the performance of the Deliverables infringes or allegedly infringes (including the defence of such infringement or alleged infringement or passing off) of any third party IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract;
"IR35"	the off-payroll rules requiring individuals who work through their company pay the same income tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies ;
"Joint Controller Agreement"	the agreement (if any) entered into between the Relevant Authority and the Supplier substantially in the form set out in Annex 2 of Joint Schedule 11 (<i>Processing Data</i>);
"Joint Controllers"	where two or more Controllers jointly determine the purposes and means of Processing;
"Joint Control"	where two or more Controllers agree jointly to determine the purposes and means of Processing Personal Data;
"Key Staff"	the individuals (if any) identified as such in the Order Form and any Statement of Work;

Joint Schedule 2 (Variation Form)

"Key Sub-Contract"	each Sub-Contract with a Key Subcontractor;
"Key Subcontractor"	<p>any Subcontractor:</p> <p>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or</p> <p>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or</p> <p>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the aggregate Charges forecast to be payable under the Call-Off Contract, and the Supplier shall list all such Key Subcontractors in section 19 of the Framework Award Form and in the Key Subcontractor Section in Order Form;</p>
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date;
"Law"	any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply;
"Location"	the place at or from which the Supplier's team will provide the Services under the Call-Off Contract and, if applicable, each SOW;
"Losses"	all losses, liabilities, damages, costs, expenses (including legal and professional fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "Loss" shall be interpreted accordingly;
"Lots"	the number of lots specified in Framework Schedule 1 (Specification), if applicable;
"Management Charge"	the sum specified in the Framework Award Form payable by the Supplier to CCS in accordance with Framework Schedule 5 (Management Charges and Information);
"Management nformation" or	the management information specified in Framework Schedule 5 (Management Charges and Information);
"Material KPIs"	are Key Performance Indicators which are identified by the Buyer as having a material impact on the performance of the Call-Off Contract;

Joint Schedule 2 (Variation Form)

"MI Default"	when two (2) MI Reports are not provided in any rolling six (6) Month period
"MI Failure"	when an MI report: a) contains any material errors or material omissions or a missing mandatory field; or b) is submitted using an incorrect MI reporting Template; or c) is not submitted by the reporting date (including where a declaration of no business should have been filed);
"MI Report"	a report containing Management Information submitted to the Authority in accordance with Framework Schedule 5 (Management Charges and Information);
"MI Reporting Template"	the form of report set out in the Annex to Framework Schedule 5 (Management Charges and Information) setting out the information the Supplier is required to supply to the Authority;
"Milestone"	an event or task described in the Implementation Plan or Statement of Work;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be Achieved;
"Misconduct"	has the meaning given to it in Paragraph 7.2 of Framework Schedule 7 (Call-Off Award Procedure);
"Month"	a calendar month and "Monthly" shall be interpreted accordingly;
"National Insurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
"New IPR"	a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same; but shall not include the Supplier's Existing IPR;
"Occasion of Tax –Compliance"	where: a) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of: i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any Tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

Joint Schedule 2 (Variation Form)

	<p>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or</p> <p>b) any Tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for Tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion;</p>
-Payroll Worker"	<p>a worker (or contractor), not employed by the Supplier or any other organisation within the supply chain, that provides their services through their own private limited company or other type of intermediary which may include the worker's own personal service company, a partnership or an individual;</p>
"Open Book Data"	<p>complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Call-Off Contract, including details and all assumptions relating to:</p> <p>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;</p> <p>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:</p> <p>i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;</p> <p>ii) staff costs broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each grade;</p> <p>iii) a list of Costs underpinning those rates for each grade, being the agreed rate less the Supplier Profit Margin; and</p> <p>iv) Reimbursable Expenses, if allowed under the Order Form; c) Overheads;</p> <p>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;</p> <p>e) the Supplier Profit achieved over the Framework Contract Period and on an annual basis;</p> <p>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;</p> <p>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and</p>

"MI" Non "Off

Joint Schedule 2 (Variation Form)

	h) the actual Costs profile for each Service Period;
"Option"	the selection of an option by the Buyer which is incorporated into the Call-Off Contract and, if applicable, any Statement of Work, which the Supplier must comply with;
"Optional Extension Period"	is the Buyer's maximum optional extension period to the Call-Off Initial Period as set out in the Order Form;
"Order"	an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract;
"Order Form"	a completed Order Form Template (or equivalent information issued by the Buyer) used to create a Call-Off Contract;
"Order Form Template"	the template in Framework Schedule 6 (Order Form Template, SOW Template and Call-Off Schedules);
"Other Contracting Authority"	any actual or potential Buyer under the Framework Contract;
"Outward Exchange"	an exchange of Supplier Staff from the Supplier to the Buyer in accordance with the Secondment Agreement;
"Overhead"	those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs";
"Parliament"	takes its natural meaning as interpreted by Law;
"Party"	in the context of the Framework Contract, CCS or the Supplier, and in the context of a Call-Off Contract the Buyer or the Supplier. "Parties" shall mean both of them where the context permits;
"Performance Indicators" or "PIs"	the performance measurements and targets in respect of the Supplier's performance of the Framework Contract set out in Framework Schedule 4 (Framework Management);
"Personal Data"	has the meaning given to it in the UK GDPR;
"Personal Data Breach"	has the meaning given to it in the UK GDPR;
"Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Relevant Authority and/or their subcontractor and/or Subprocessor (as detailed in Joint Schedule 11 (Processing Data)) engaged in the performance of its obligations under a Contract;
"Place of Performance"	the place or location at which the Deliverables, in whole or part, shall be performed;

Joint Schedule 2 (Variation Form)

"Platform"	the platform, site or system (also known as 'Contract-a-Thing') operated on behalf of CCS which requires a potential Buyer to complete the Buyer Registration Procedure and specify its Authorised
	Users who may access and use the platform, site or system on behalf of the Buyer and use it to assist in selecting or shortlisting suppliers when undertaking a Call-Off Procedure in accordance with Framework Schedule 7, to Order Deliverables under a Contract;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies ;
"Pricing Matrix"	the pricing matrix of the Supplier may be found in the Platform and also in Annex 1 (Pricing Matrix) of Framework Schedule 3 (Framework Prices) which sets out the maximum Day Rates for each DDaT role for all Supplier Staff under the Contract;
"Pricing Mechanism"	the pricing mechanisms are (a) Capped Time and Materials, (b) Incremental Fixed Prices, (c) Time and Materials, (d) Fixed Price, and (e) a combination of two or more of these as set out in Framework Schedule 3 (Framework Prices) and Framework Schedule 7 (Call-Off Award Procedure) and as may be refined in the Further Competition Procedure;
"Pricing Tool"	the tool to be used by Buyers as part of the Call-Off Procedure which is set out in Annex D (Pricing Tool) of Framework Schedule 7 (Call-Off Award Procedure);
"Processing"	has the meaning given to it in the UK GDPR;
"Processor"	has the meaning given to it in the UK GDPR;
"Progress Meeting"	a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative;
"Progress Meeting Frequency"	the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form;
"Progress Report"	a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates;
"Progress Report Frequency"	the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form;

Joint Schedule 2 (Variation Form)

"Prohibited Acts"	<p>a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:</p> <ul style="list-style-type: none"> i) induce that person to perform improperly a relevant function or activity; or ii) reward that person for improper performance of a relevant function or activity; <p>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for</p>
	<p>improper performance of a relevant function or activity in connection with each Contract; or</p> <p>c) committing any offence:</p> <ul style="list-style-type: none"> i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or ii) under legislation or common law concerning fraudulent acts; or iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or <p>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK;</p>
"Protective Measures"	<p>appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Framework Schedule 9 (Cyber Essentials Scheme), if applicable, in the case of the Framework Contract or Call-Off Schedule 9 (Security), if applicable, in the case of a Call-Off Contract.</p>
"Recall"	<p>a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance;</p>
"Recipient Party"	<p>the Party which receives or obtains directly or indirectly Confidential Information;</p>

Joint Schedule 2 (Variation Form)

"Rectification Plan"	the Supplier's plan (or revised plan) to rectify it's breach using the template in Joint Schedule 10 (Rectification Plan) which shall include: a) full details of the Default that has occurred, including a root cause analysis; b) the actual or anticipated effect of the Default; and c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable);
"Rectification Plan Process"	the process set out in Clause 10.3.1 to 10.3.4 (Rectification Plan Process);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires);
"Reimbursable Expenses"	the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance
	with the Buyer's expenses policy current from time to time, but not including: a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;
"Relevant Authority"	the Authority which is party to the Contract to which a right or obligation is owed, as the context requires;
"Relevant Authority's Confidential information"	a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR); b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and c) information derived from any of the above;
"Relevant Requirements"	all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010;
"Relevant Tax Authority"	HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established;

Joint Schedule 2 (Variation Form)

"Reminder Notice"	a notice sent in accordance with Clause 10.5 given by the Supplier to the Buyer providing notification that payment has not been received on time;
"Replacement Deliverables"	any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Call-Off Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Subcontractor"	a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor);
"Replacement Supplier"	any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer;
"Request For Information"	a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs;
"Required Insurances"	the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form;
"Resource"	the Buyer shall issue the Supplier and all Key Staff who are Off-Payroll Workers with a Status Determination Statement describing the IR35 status of each Supplier Staff in a key role or position being engaged to provide Services under the Contract;
"Resource Profile"	the capacity of the Supplier to provide various DDaT roles aggregated at Role Family level and is designed to understand what skills are available from the Supplier and any named Subcontractors in terms of approximate number of Supplier Staff and the level of security clearance that must have been obtained by the Supplier Staff prior to commencement on a relevant Call-Off Contract;
"Restricted Staff"	any person employed or engaged by either Party, in the capacity of director or in any research, technical, IT, security, engineering, procurement, financial, legal or managerial role who has been engaged in the provision of the Deliverables or management of the Contract either as principal, agent, employee, independent contractor or in any other form of employment or engagement over the previous 12 Months, directly worked with or had any material dealings, but shall not include any person employed or engaged in an administrative, clerical, manual or secretarial capacity;
"Retained EU Law"	the category of UK Law created under Section 2 to 4 of the European Union (Withdrawal) Act 2018 at the end of the transition period following the repeal of the savings to the European Communities Act 1972;

Joint Schedule 2 (Variation Form)

"Request for Information" or "RFI" Tool	the functional tool within the Platform (or as otherwise described in Framework Schedule 7 (Call-Off Award Procedure) to be used by Buyers to seek clarification or additional information from one or more suppliers that will assist the Buyer in preparing its Statement of Requirement, planning and conducting its Call-Off Procedure ,before undertaking a Call-Off Procedure in accordance with Framework Schedule 7 (Call-Off Award Procedure);
"Role Family"	the grouping of related roles or professions which share common skills and capabilities;
"Satisfaction Certificate"	the certificate (materially in the form of the document contained in of Part B of Call-Off Schedule 13 (Implementation Plan and Testing) or as agreed by the Parties where Call-Off Schedule 13 is not used in this Contract) granted by the Buyer when the Supplier has met all of the requirements of an Order, Achieved a Milestone or a Test;
"Scalability"	the potential size of the Supplier team needed to fulfil the Buyer requirements;
"Secondment"	the temporary transfer of one or more Supplier Staff from the Supplier to the Buyer to another position or employment, in accordance with the Secondment Agreement for the Secondment Charge; and "Secondee" is a person on a Secondment;

"Secondment Agreement"	the agreement entered into between the Supplier and Buyer regarding an Inward Exchange or an Outward Exchange or a Secondment which shall be in the form and format of the Call-Off Schedule 26 (Secondment Agreement Template);
"Secondment Charge"	the Charge for Supplier Staff on an Outward Secondment which shall be no more than the base salary and any relevant pension contributions ordinarily payable by the Supplier in respect of a Secondee (inclusive of VAT);
"Security Management Plan"	the Supplier's security management plan prepared pursuant to Call-Off Schedule 9 (Security) (if applicable);
"Security Policy"	the Buyer's security policy, referred to in the Order Form, in force as at the Call-Off Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier;
"Self Audit Certificate"	the certificate in the form as set out in Framework Schedule 8 (Self Audit Certificate);
"Serious Fraud Office"	the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time;

Joint Schedule 2 (Variation Form)

"Service Capability"	the Service capabilities of the Supplier as set out in Annex 2 of Framework Schedule 1 (Specification) which are grouped under the following headings under which there are a number of subcapabilities: 1. Performance analysis and data; 2. Security; 3. Service delivery; 4. Software development; 5. Support and operations; 6. Testing and auditing; 7. User experience; and 8. User research;
"Service Levels"	any service levels applicable to the provision of the Deliverables under the Call Off Contract (which, where Call Off Schedule 14 (Service Levels) is used in this Contract, are specified in the Annex to Part A of such Schedule);
"Service Period"	has the meaning given to it in the Order Form;
"Service Provision"	one or more of the service provisions set out in Paragraph 1.1 of Framework Schedule 1 (Specification);

"Services"	services made available by the Supplier as specified in Framework Schedule 1 (Specification) and in relation to a Call-Off Contract as specified in the Order Form and each Statement of Work;
"Service Transfer"	any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor;
"Service Transfer Date"	the date of a Service Transfer;
"Sites"	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;
"SME"	an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises;
"Special Terms"	any additional Clauses set out in the Framework Award Form or Order Form which shall form part of the respective Contract;

Joint Schedule 2 (Variation Form)

"Specific Change in Law"	a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date;
"Specification"	the specification set out in Framework Schedule 1 (Specification), as may, in relation to a Call-Off Contract, be supplemented by the Order Form and, if applicable, each Statement of Work;
"Standards"	any: a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with; b) standards detailed in the specification in Schedule 1 (Specification); c) standards detailed by the Buyer in the Order Form, Statement of Work or agreed between the Parties from time to time; d) relevant Government codes of practice and guidance applicable from time to time;
"Start Date"	in the case of the Framework Contract, the date specified on the Framework Award Form, and in the case of a Call-Off Contract, the

	date specified in the Order Form, and in the case of a Statement of Work, the date specified in that Statement of Work;
"Statement of Requirements"	a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Call-Off Procedure;
"Statement of Work" or "SOW"	the document which, upon execution by the Buyer and Supplier, shall become incorporated into their Call-Off Contract and it outlines the agreed body of works to be undertaken as part of the Call-Off Contract Deliverables. There may be any number of Statements of Work incorporated into a Call-Off Contract and each Statement of Work may include (but is not limited to) the Statement of Requirements, identified output(s), completion date(s) and charging method(s);
"Status Determination Statement" or "SDS"	a statement that describes the determination reached by the Buyer/client on the employment status (i.e. IR35 status) of an OffPayroll Worker for a particular Call-Off Contract or any element of work undertaken as part of any SOW, and the reasons for reaching that determination. The SDS must be passed to the worker and the person or organisation the client contracts with for the worker's services;
"SOW End Date"	the date up to and including this date when the supply of the Deliverables under the Statement of Work shall cease
"SOW Start Date"	the date of the start of the Statement of Works as stated in the SOW;

Joint Schedule 2 (Variation Form)

"Storage Media"	the part of any device that is capable of storing and retrieving data;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than a Call-Off Contract or the Framework Contract, pursuant to which a third party: a) provides the Deliverables (or any part of them); b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third Party appointed to process Personal Data on behalf of that Processor related to a Contract;
"Summary of Work"	a short description of overview of the Buyer's Statement of Requirements;
"Supplier"	the person, firm or company identified in the Framework Award Form;
"Supplier Assets"	all assets and rights used by the Supplier to provide the Deliverables in accordance with the Call-Off Contract but excluding the Buyer Assets;
"Supplier Authorised Representative"	the representative appointed by the Supplier named in the Framework Award Form, or later defined in a Call-Off Contract;
"Supplier Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Supplier's Confidential Information"	a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier; b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract; c) Information derived from any of (a) and (b) above;
"Supplier's Contract Manager"	the person identified in the Order Form appointed by the Supplier to oversee the operation of the Call-Off Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment;

Joint Schedule 2 (Variation Form)

"Supplier Equipment"	the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Call-Off Contract;
"Supplier Marketing Contact"	shall be the person identified in the Framework Award Form;
"Supplier Non-Performance"	where the Supplier has failed to: a) Achieve a Milestone by its Milestone Date; b) provide the Goods and/or Services in accordance with the Service Levels; and/or c) comply with an obligation under a Contract;
"Supplier Profit"	in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of a Call-Off Contract for the relevant period;
"Supplier Profit Margin"	in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract;
"Supporting Documentation"	sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Call-Off Contract detailed in the information are properly payable;

Tax"	a) all forms of taxation whether direct or indirect; b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
Termination Notice"	a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination;

Joint Schedule 2 (Variation Form)

Test Issue"	any variance or non-conformity of the Deliverables from their requirements as set out in a Call-Off Contract;
Test Plan"	a plan: a) for the Testing of the Deliverables; and b) setting out other agreed criteria related to the achievement of Milestones;
Tests "	any tests required to be carried out pursuant to a Call-Off Contract as set out in the Test Plan or elsewhere in a Call-Off Contract and "Tested" and "Testing" shall be construed accordingly;
Third Party IPR"	Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
Time and Materials"	a Pricing Mechanism whereby the Buyer agrees to pay the Supplier for the work performed by the Supplier Staff, based on no more than the pro rata division of the Day Rates by 7.5 to provide an Hourly Rate for the applicable grade of Supplier Staff who undertook the work (as set out in Annex 1 of Framework Schedule 3 (Framework Prices)) and for the materials used in the project based on pre-agreed material disclosures and subject to time approval by the Buyer;
Transferring Supplier Employees"	those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date;

"Transparency Information"	the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for – a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and b) Commercially Sensitive Information;
"Transparency Reports"	the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Call-Off Schedule 1 (Transparency Reports);
"UK GDPR"	the Retained EU Law version of the General Data Protection Regulation (Regulation (EU) 2016/679);
"User Terms"	the terms of use applicable to all Buyer's Authorised Users who access and use the Platform which are available at: [Insert link] ;
"Variation"	any change to a Contract, including any change to a SOW under a CallOff Contract;
"Variation Form"	the form set out in Joint Schedule 2 (Variation Form);
"Variation Procedure"	the procedure set out in Clause 24 (Changing the contract);

Joint Schedule 2 (Variation Form)

"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"VCSE"	a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables;
"Worker Engagement Status"	the details of the labour supply chain through which the Worker is engaged as Supplier Staff, for example, the Worker could be: (a) "employed by the Supplier the Buyer contracts with"; (b) "employed by another organisation within the supply chain, e.g. an agency or umbrella company"; (c) "an off-payroll worker engaged via an intermediary e.g. the worker's own personal service company"; or (d) "an independent sole trader";
"Working Day"	any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form;
"Work Day"	a minimum of 7.5 Work Hours, whether or not such hours are worked consecutively and whether or not they are worked on the same day; and
"Work Hours"	the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks.

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 below]	[insert detail here or use Annex 1
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:
	<input type="checkbox"/> [CCS/Buyer to insert] original Clauses or Paragraphs to be varied and the changed clause]
	<input type="checkbox"/> [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]

Joint Schedule 2 (Variation Form)

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. 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

ANNEX 1

[insert] details as required

**Joint Schedule 2 (Variation
Form)**

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 nonrenewal 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)

1. What is the Commercially Sensitive Information?

- 1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.
- 1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).
- 1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Item(s)	Duration of Confidentiality
1	Call-Off Schedule 4 (Call Off Tender)	In perpetuity
2	Call-Off Schedule 5 - Pricing Details and expenses policy	In perpetuity
3	Framework Schedule 6 (Order Form template and call-off schedules) Pricing, Key staff, and named individuals and contact details	In perpetuity

Joint Schedule 7 (Financial Difficulties)

5	Tender response	In perpetuity
6	Any supplementary information provided to the client in relation to the Call-Off Schedules and Joint Schedules e.g., BCDR plan, security information, key personnel, testing audit and reports	In perpetuity

Joint Schedule 5 (Corporate Social Responsibility)

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 available 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

Joint Schedule 7 (Financial Difficulties)

- 3.1.3 employer and shall be free to leave their employer after reasonable notice;
- 3.1.4 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;

Joint Schedule 7 (Financial Difficulties)

- (b) frequency; and
 - (c) hours worked;
- by individuals and by the Supplier Staff as a whole;
- 1.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.
- 1.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:
 - 1.3.1 this is allowed by national law;
 - 1.3.2 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
 - 1.3.3 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.
- 1.4 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.

2. Sustainability

- 2.1 The Supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:
<https://www.gov.uk/government/collections/sustainable-procurement-thegovernment-buying-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 subcontract its obligations under each Call-Off Contract to the Key Subcontractors set out in the Call-Off Order Form.
- 1.2 Subject to Paragraph 1.1, the Supplier is entitled to sub-contract some of 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 Sub-Contract 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 the 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;

Joint Schedule 7 (Financial Difficulties)

- 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 SubContract 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 SubContract 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 subcontract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract 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):

"Credit Rating Threshold"	1 the minimum credit rating level for the Monitored Company as set out in Annex 2 and
"Financial Distress Event"	2 the occurrence or one or more of the following events: <ul style="list-style-type: none">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; orf) any of the following:<ul style="list-style-type: none">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;

Joint Schedule 7 (Financial Difficulties)

	<ul style="list-style-type: none">iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; oriv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company
	3 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"	4 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"	5 Supplier REDACTED TEXT under FOIA Section 40, Personal Information , The Supplier parent company and any Key Subcontractor
"Rating Agencies"	6 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 1:
Framework Ref: RM6260
Project Version: v1.0

**Joint Schedule 7 (Financial
Difficulties)**

auditors thereafter provide CCS within 10 Working Days of the end of each

Joint Schedule 7 (Financial Difficulties)

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.

3.4The 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.

3.5For 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

4.1In 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.

4.2In 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.]

4.3The 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

Joint Schedule 7 (Financial Difficulties)

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;
- 5.1.3 in the case of the Buyer, the Supplier fails to agree a Financial Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) that ensures the continued performance of the Contract and delivery of the Deliverables under its Contract; and/or
- 5.1.4 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.

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")

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit Rating (long Term)	Credit Rating Threshold

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]

Joint Schedule 10 (Rectification Plan)

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)

Definitions

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

**“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:

Joint Schedule 10 (Rectification Plan)

- (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.
-

Joint Schedule 10 (Rectification Plan)

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*

Joint Schedule 10 (Rectification Plan)

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 UK 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.

Joint Schedule 10 (Rectification Plan)

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

Joint Schedule 10 (Rectification Plan)

- (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

Joint Schedule 10 (Rectification Plan)

- (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.

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;
- Framework Ref:
RM6263
Project Version: v1.0

Joint Schedule 10 (Rectification Plan)

- (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
-

Joint Schedule 10 (Rectification Plan)

- (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.

**Joint Schedule 10 (Rectification
Plan)**

Annex 1 - Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

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

1.

1.1.1.1 The contact details of the Supplier's Data Protection Officer are:

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

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

Description	Details
Identity of Controller for each Category of Personal Data	<p>The Relevant Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 3 to paragraph 16 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none">• See 'type of personal data' for specific attributes.• Special categories include: race, health data, sex life and sexual orientation.
Duration of the Processing	<i>For the duration of the services.</i>
Nature and purposes of the Processing	<ul style="list-style-type: none">• Design and build of the IBCA data platform• Reviewing data about the person making a claim to:• Understand existing support scheme claim and payments• Review evidence to support the claim• Enable subsequent assessment by an IBCA Claims Manager re: eligibility for compensation, where such a claim is made - or for claims yet to be made• Determination and delivery by an IBCA Claims Manager of registered estate compensation.• Determination, registration and delivery of compensation by an IBCA Claims Manager for unregistered people (infected, affected & estates) eligible to claim for compensation

Joint Schedule 10 (Rectification Plan)

	<ul style="list-style-type: none"> Alert, monitor, and report to enable IBCA personnel to act on possible fraud and error for a person, or a claim.
Type of Personal Data	<p><u>For persons making a claim</u></p> <p>Type of person making a claim (infected or affected)</p> <p>Personal Information:</p> <ul style="list-style-type: none"> Title Full Name <ul style="list-style-type: none"> First Name Middle Name Surname Suffix Date of birth Date of death Cause of death Sex at birth Preferred name <p>Contact / ID Information:</p> <ul style="list-style-type: none"> Contact address National Insurance number NHS number Contact number Email address Preferred contact method Preferred contact times Accessibility requirements <p>Infection context:</p> <ul style="list-style-type: none"> NHD number Diagnosis Haemophilia centre Date first seen Deficiency factor Deficiency severity Infection data Diagnosis date Test/screening outcomes Treatment year & quarter Blood products administered <p>Associated Person Personal Details:</p> <ul style="list-style-type: none"> Next of Kin Dependent children <p>Probate Information</p>

Joint Schedule 10 (Rectification Plan)

	<ul style="list-style-type: none"> • Estate beneficiary <p>Claim Information:</p> <ul style="list-style-type: none"> • IBSS scheme registration number • Claim reference number • Start date for IBCA claim • Claim Status • Claim Manager
Categories of Data Subject	<ul style="list-style-type: none"> • Customers <ul style="list-style-type: none"> ○ those claiming, their representatives and their relatives ○ medical clinicians and healthcare works associated with those claiming • Staff (claim managers)
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	<p>All processing of personal data by the Supplier will be undertaken on IT provided by the Authority.</p> <p>No plan for return and destruction is required as a result of personal data processing being undertaken by the Supplier within Authority infrastructure.</p>

Joint Schedule 13 (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):
- | | |
|---|--|
| "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 can be found at: |
| "Cyber Essentials Basic Certificate" | https://www.cyberessentials.ncsc.gov.uk/ the certificate awarded on the basis of selfassessment, 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 Framework Award Form and/or Order Form requires that the Supplier provide a Cyber Essentials Plus Certificate prior to Framework Start Date and/or commencing the provision of Deliverables under the Call-Off Contract including, if applicable, any Statement of Work, the Supplier shall provide a valid Cyber Essentials Plus Certificate to CCS and/or 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 CCS and/or 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 CCS and/or the Buyer evidence of renewal of the 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, CCS and/or the Buyer reserves the right to terminate the Call-Off Contract for material Default.

Joint Schedule 10 (Rectification Plan)

- 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 Plus Scheme under Paragraph 2.1 of this Schedule.
- 2.5 This Schedule shall survive termination or expiry of this Contract and each and any Call-Off Contract.



Cabinet Office

Commercial Information Assurance Team

Security Management Plan Template Developer Schedule
[Project/Service and Supplier Name]

Dated

2024

Contents

1	Executive summary	1
2	System description	1
3	Risk assessment	3
4	In-service controls.....	4
5	Supply chain security and third party subcontractors/tools	5
6	Personnel security	5
7	Business continuity	5
8	Physical security	6
9	Incident management process	6

APPENDICES

APPENDIX 1 ISO27001 AND/OR CYBER ESSENTIAL PLUS CERTIFICATES APPEN-
DIX 2 CLOUD SECURITY PRINCIPLES ASSESSMENT
APPENDIX 3 PROTECTING BULK DATA ASSESSMENT IF REQUIRED BY THE AU-
THORITY/CUSTOMER
APPENDIX 4 LATEST ITHC REPORT AND VULNERABILITY CORRECTION PLAN AP-
PENDIX 5 STATEMENT OF APPLICABILITY

Joint Schedule 10 (Rectification Plan)

1 Executive summary

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

1.1 Change history

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

1.2 References, links and dependencies

ID	Document Title	Reference	Date

1.3 Supplier personnel

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

2 System description

2.1 Background

[A short description of the project/product/system being developed. Describe its purpose, functionality, aim and scope. If the system is to be managed by the Supplier once developed then details should be included of the scope of that work and this SMP will need to be updated once the core development activity has been completed.]

2.2 Organisational Ownership/Structure

[Who owns the system and will operate the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance eg how a Security

**Joint Schedule 10 (Rectification
Plan)**

Working Group reports to the project board.]

Joint Schedule 10 (Rectification Plan)

2.3 Information assets and flows

- (a) Logical data flow diagram

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

- (b) Data assets

[Include a table of the type and volumes of data that will be processed, managed and stored within the developed system. If personal data, please include the fields used such as name, address, department DOB, NI number etc. Details of any test data and whether live or anonymised. Data processed by third party suppliers must be included here]

2.4 System architecture

[A description of the proposed physical system architecture, to include any cloud services and the system management. Please provide a diagram if helpful.]

2.5 Users and Sub-contractors

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

2.6 Register of Support Locations and Third-Party Tools

[Please provide a table of the nature of the activity performed at the support location, where the activity will be undertaken, where any Authority data assets will be stored and processed and any locations they will be managed from. This must include the locations of any help desks or call centres if relevant. All third-party suppliers, subcontractors and third-party tools must be included in this section. Any off-shoring considerations should be detailed with the legal basis for any data transfer included e.g. International Data Transfer Agreements, equivalency etc.]

2.7 Certifications

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

2.8 Test and development systems

[Include information about any test, development, pre-production and user acceptance testing systems, their locations and whether they contain live system data.]

2.9 Modules Register

Joint Schedule 10 (Rectification Plan)

[*Include a table of all Third-party Software Modules that form part of the Code. This must include the name of the developer, the due diligence undertaken by the supplier, any recognised security vulnerabilities and how the supplier will minimise the effect of those.*]

2.10 Support Register

[A table should be included of all software used in the development activity, the date it will cease to be in mainstream support]

3 Risk assessment

3.1 Accreditation/assurance scope

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

3.2 Risk appetite

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

3.3 Business impact assessment

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

3.4 Risk assessment

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

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

Joint Schedule 10 (Rectification Plan)

R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low
----	---	--------	---	--	----------

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are logged and audited. C14. Letters are automatically sent to users home addresses when bank details are altered. C15. Staff awareness training	Low

3.5 Controls

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

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC

Joint Schedule 10 (Rectification Plan)

C1 5	Staff awareness training	All staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO27001 certification
---------	--------------------------	---	---

3.6 Residual risks and actions

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

4 In-service controls

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

4.1 Protective monitoring

Joint Schedule 10 (Rectification Plan)

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

4.2 Malware prevention

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

4.3 End user devices

[This section should detail the security controls which are implemented on all fixed and removable end user devices used to process, store or manage Authority data against the end-user device requirements in the contract.]

4.4 Encryption

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

4.5 Vulnerability management

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

4.6 Identity, verification and access controls

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

4.7 Data Deletion

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

5 Supply chain security and third party subcontractors/tools

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

6 Personnel security

[Please provide details of your Personnel Security Vetting Policy for those staff who will have access to, or come into contact with Buyer data or assets.

Please provide details of how you will ensure that all staff accessing Buyer data are aware of the confidential nature of the data and comply with their

Joint Schedule 10 (Rectification Plan)

legal and specific obligations under the Contract?]

7 Business continuity

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

8 Physical security

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

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

9 Incident management process

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

**Joint Schedule 10 (Rectification
Plan)**

Appendix 1 ISO27001 and/or cyber essential plus certificates

[Please include copies of the certificates here]

Appendix 2 Cloud security principles assessment

[Please add your controls in the attached table.]

Principle	Goals of the Principle	Controls
Principle 1 – Data in transit protection "User data transiting networks should be adequately protected against tampering and eavesdropping."	<ul style="list-style-type: none">• Data in transit is protected between end user device(s) and the service• Data in transit is protected internally within the service• Data in transit is protected between the service and other services (eg where APIs are exposed)	
Principle 2 – Asset protection and resilience "User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure."	Cloud service consumers should seek to understand: <ul style="list-style-type: none">• In which countries their data will be stored, processed and managed. They should also consider how this affects compliance with relevant legislation e.g. Data Protection Act (DPA), GDPR etc.• Whether the legal jurisdiction(s) within which the service provider operates are acceptable to them	
Principle 3 – Separation between users "A malicious or compromised user of the service should not be able to affect the service or data of another."	Cloud service consumers should seek to: <ul style="list-style-type: none">• Understand the types of user they share the service or platform with• Have confidence that the service provides sufficient separation of their data and service from other users of the service• Have confidence that management of their service is kept separate from other users (covered separately as part of Principle 9)	

Joint Schedule 10 (Rectification Plan)

Principle	Goals of the Principle	Controls
<p>Principle 4 – Governance framework</p> <p>"The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined."</p>	<p>Cloud service consumers should ensure that:</p> <ul style="list-style-type: none"> • A clearly identified, and named, board representative (or a person with the direct delegated authority) is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer' • A documented framework exists for security governance, with policies governing key aspects of information security relevant to the service • Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk • Processes to identify and ensure compliance with applicable legal and regulatory requirements have been established 	
<p>Principle 5 – Operational security</p> <p>"The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes."</p>	<p>Cloud service consumers should be confident that:</p> <ul style="list-style-type: none"> • The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime • Changes to the service are assessed for potential security impact. Then managed and tracked through to completion 	
<p>Principle 6 – Personnel security</p> <p>"Where service provider personnel have access to</p>	<p>Cloud service consumers should be confident that:</p> <ul style="list-style-type: none"> • The level of security screening conducted on 	

Joint Schedule 10 (Rectification Plan)

Principle	Goals of the Principle	Controls
your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel."	<p>service provider staff with access to the consumers information, or with ability to affect the service, is appropriate</p> <ul style="list-style-type: none"> The minimum number of people necessary have access to the consumers information or could affect the service 	
<p>Principle 7 – Secure development</p> <p>"Services should be designed and developed to identify and mitigate threats to their security.</p> <p>Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity."</p>	<p>Cloud service consumers should be confident that:</p> <ul style="list-style-type: none"> New and evolving threats are reviewed, and the service improved in line with them Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment 	
<p>Principle 8 – Supply chain security</p> <p>"The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement."</p>	<p>Cloud service consumers should seek to understand and accept:</p> <ul style="list-style-type: none"> How their information is shared with, or accessible to, third party suppliers and their supply chains How the service provider's procurement processes place security requirements on third party suppliers How the service provider manages security risks from third party suppliers How the service provider manages the conformance of their suppliers with security requirements How the service 	

Joint Schedule 10 (Rectification Plan)

	provider verifies that hardware and	
--	-------------------------------------	--

Principle	Goals of the Principle	Controls
	software used in the service is genuine and has not been tampered with	
Principle 9 – Secure user management "Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data."	Cloud service consumers should: <ul style="list-style-type: none"> • Be aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.) • Ensure that only authorised individuals from their organisation can use those mechanisms to affect their use of the service (Principle 10 can help consumers consider the strength of user identification and authentication in each of these mechanisms) 	

Joint Schedule 10 (Rectification Plan)

Principle 10 – Identity and authentication "All access to service interfaces should be constrained to authenticated and authorised individuals."	Cloud service consumers should: <ul style="list-style-type: none"> • Have confidence that identity and authentication controls ensure users are authorised to access specific interfaces 	
Principle 11 – External interface protection "All external or less trusted interfaces of the service should be identified and appropriately defended."	Cloud service consumers should: <ul style="list-style-type: none"> • Understand what physical and logical interfaces their information is available from, and how access to their data is controlled • Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10) 	

Principle	Goals of the Principle	Controls
Principle 12 – Secure service administration "Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data."	Cloud service consumers should: <ul style="list-style-type: none"> • Understand which service administration model is being used by the service provider to manage the service • Be content with any risks the service administration model in use brings to the consumers data or use of the service 	

Joint Schedule 10 (Rectification Plan)

<p>Principle 13 – Audit information for users</p> <p>"You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales."</p>	<p>Cloud service consumers should:</p> <ul style="list-style-type: none">• Be aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it• Be confident that the audit information available will meet their needs for investigating misuse or incidents	
<p>Principle 14 – Secure use of the service</p> <p>"The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected."</p>	<p>Cloud service consumers should:</p> <ul style="list-style-type: none">• Understand any service configuration options available to them and the security implications of their choices• Understand the security requirements of their use of the service• Educate their staff using and managing the service in how to do so safely and securely	

**Joint Schedule 10 (Rectification
Plan)**

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

[A spreadsheet may be attached]

**Joint Schedule 10 (Rectification
Plan)**

Appendix 4 Latest ITHC report and vulnerability correction plan

Appendix 5 Statement of applicability

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

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	<input checked="" type="checkbox"/>
	a standard agreement	<input type="checkbox"/>
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	<input checked="" type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
	No certification required	<input type="checkbox"/>
The Supplier must ensure that Higher-risk Sub-contractors have the following Certifications (or equivalent):	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
	No certification required	<input type="checkbox"/>
The Supplier must ensure that Medium-risk Sub-contractors have the following Certifications (or equivalent):	Cyber Essentials Plus	<input type="checkbox"/>
	Cyber Essentials	<input type="checkbox"/>
	No certification required	<input type="checkbox"/>
Buyer Security Policies (see Paragraph 6)		
The Buyer requires the Supplier to comply with the following policies relating to security management: Buyers suppliers Management policy		<input type="checkbox"/>
Secure by Design Questionnaire (Paragraph 12)		
The Buyer requires the Supplier to complete the Secure by Design Questionnaire		<input type="checkbox"/>
Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Sub-contractors may store, access or Handle Government Data	the United Kingdom only	<input checked="" type="checkbox"/>

Joint Schedule 10 (Rectification Plan)

in:	any territory as permitted by and in accordance with any regulations for	<input type="checkbox"/>
-----	--	--------------------------

	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	<input type="checkbox"/>
Support Locations (see Paragraph 1 of the Security Requirements)		
The Supplier and Subcontractors may operate Support Locations in:	the United Kingdom only	<input checked="" type="checkbox"/>
	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)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>
Locations for Development Activity (see Paragraph 1 of the Security Requirements)		<input type="checkbox"/>
The Supplier and Subcontractors may undertake Development Activity in:	the United Kingdom only	<input checked="" type="checkbox"/>
	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)	<input type="checkbox"/>
	anywhere in the world not prohibited by the Buyer	<input type="checkbox"/>

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 [◆] (*Security Management*).
- 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 [◆] (*Security Management*) 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 [♦] (*Security Management*):

“Anti-virus Software”	means software that: <ul style="list-style-type: none"> (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: <ul style="list-style-type: none"> (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 Buyer 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: <ul style="list-style-type: none"> (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 Buyer 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 Buyer 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: <ul style="list-style-type: none"> (i) Supplier Information Management System; (ii) Development Environment; or (iii) Developed System;

	<p>(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:</p> <p>(i) Supplier Information Management System;</p> <p>(ii) Development Environment; or</p> <p>(iii) Developed System; and</p> <p>(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:</p> <p>(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or</p> <p>(ii) was undertaken, or directed by, a state other than the United Kingdom;</p>
“Buyer Data”	<p>means any:</p> <p>(a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media;</p> <p>(b) Personal Data for which the Buyer is a, or the, Data Controller; or</p> <p>(c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b);</p> <p>that is:</p> <p>(a) supplied to the Supplier by or on behalf of the Buyer; or</p> <p>(b) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract; and</p> <p>for the avoidance of doubt includes the Code and any meta-data relating to the Code;</p>
“Buyer Data Register”	means the register of all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer, produced and maintained in accordance with Paragraph 24 of the Security Requirements;
“Buyer Equipment”	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;
“Buyer System”	<p>means the Buyer’s information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that:</p> <p>(a) is used by the Buyer or the Supplier in connection with this contract;</p> <p>(b) interfaces with the Supplier System; and/or</p> <p>(c) is necessary for the Buyer to receive the Services;</p>

“Certification Default”	means the occurrence of one or more of the circumstances listed in Paragraph 10.4;
“Certification Rectification Plan”	means the plan referred to in Paragraph 10.5(a);
“Certification Requirements”	means the requirements set out in Paragraph 10.3;
“CHECK Scheme”	means the NCSC’s scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;
“CHECK Service Provider”	means a company which, under the CHECK Scheme: <ul style="list-style-type: none"> (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;
“Code”	means, in respect of the Developed System: <ul style="list-style-type: none"> (a) the source code; (b) the object code; (c) third-party components, including third-party coding frameworks and libraries; and (d) all supporting documentation;
“Code Review”	means a periodic review of the Code by manual or automated means to: <ul style="list-style-type: none"> (a) identify and fix any bugs; and (b) ensure the Code complies with: <ul style="list-style-type: none"> (i) the requirements of this Schedule [♦] (<i>Security Management</i>); 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: <ul style="list-style-type: none"> (g) coding; (h) testing; (i) code storage; and (j) 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 Sub-contractor 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 https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html ;
“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 Sub-contractor”	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 Personnel 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-baseline-personnel-security-standard), as that document is updated from time to time;
ISO Certification	means either of the following certifications when issued by a UKAS-recognised Certification Body: <ul style="list-style-type: none"> (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;
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"Medium-risk Sub-contractor"	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 Security Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance ;
"NCSC Protecting Bulk Personal Data Guidance"	means the NCSC's document "Protecting Bulk Personal Data", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data ;
"NCSC Secure Design Principles"	means the NCSC's document "Secure Design Principles", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles ;
"OWASP"	means the Open Web Application Security Project Foundation;
"OWASP Secure Coding Practice"	means the Secure Coding Practices Quick Reference Guide published by OWASP, as updated or replaced from time to time and found at https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/ ;
"OWASP Top Ten"	means the list of the most critical security risks to web applications published annually by OWASP and found at https://owasp.org/www-project-top-ten/ ;

“Privileged User”	means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges;
“Prohibited Activity”	means the storage, access or Handling of Buyer 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 Buyer 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”	<p>means document setting out, in respect of Support Locations and Third-party Tools:</p> <ul style="list-style-type: none"> (a) the nature of the activity performed at the Support Location or by the Third-party Tool on the Code or the Buyer Data (as applicable); (b) where that activity is performed by individuals, the place or facility from where that activity is performed; and (c) in respect of the entity providing the Support Locations or Third-party Tools, its: <ul style="list-style-type: none"> (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”	<p>means:</p> <ul style="list-style-type: none"> (a) for the Supplier: <ul style="list-style-type: none"> (i) in the case of a higher-risk agreement <ul style="list-style-type: none"> (A) either: <ul style="list-style-type: none"> (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

	<p>Certification, that ISO Certification; and</p> <p>(B) Cyber Essentials Plus;</p> <p>(ii) in the case of a standard agreement, either:</p> <p>(C) the certification selected by the Buyer in Paragraph 1; or</p> <p>(D) where the Buyer has not selected a certification option, Cyber Essentials; and</p> <p>(b) for Higher-risk Subcontractors and Medium-risk Subcontractors, either:</p> <p>(i) the certification selected by the Buyer in Paragraph 1; or</p> <p>(ii) where the Buyer has not selected a certification option, Cyber Essentials,</p> <p>(or equivalent certifications);</p>
“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 Personnel 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 Personnel 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 Annex 4 (<i>Secure by Design Questionnaire</i>), 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 Guidance”	<p>means:</p> <ul style="list-style-type: none"> (a) the NCSC’s document “Secure development and deployment guidance” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/developers-collection; and (b) the OWASP Secure Coding Practice as updated or replaced from time to time;
“Security Management Plan”	means the document prepared in accordance with the requirements of Paragraph 11 and in the format, and containing the information, specified in Annex 2;
“SMP Sub-contractor”	<p>means a Sub-contractor with significant market power, such that:</p> <ul style="list-style-type: none"> (a) they will not contract other than on their own contractual terms; and (b) either: <ul style="list-style-type: none"> (i) there are no other substitutable suppliers of the particular services other than SMP Sub-contractors; or (ii) the Sub-contractor concerned has an effective monopoly on the provision of the Services;
“Sites”	<p>means any premises:</p> <ul style="list-style-type: none"> (a) from or at which: <ul style="list-style-type: none"> (i) the Services are (or are to be) provided; or (ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: <ul style="list-style-type: none"> (i) any part of the Supplier Information Management System is situated; or (ii) any physical interface with the Buyer System takes place; and (c) for the avoidance of doubt include any premises at which Development Activities take place;
“Sub-contractor”	<p>means, in this Schedule [♦] (<i>Security Management</i>), any individual or entity that:</p> <ul style="list-style-type: none"> (a) forms part of the supply chain of the Supplier; and (b) has access to, hosts, or performs any operation on or in respect of the Supplier Information Management System, the Development Environment, the Code and the Buyer Data;

“Sub-contractor Personnel”	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (b) engaged in or likely to be engaged in: (i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services;
“Supplier Information Management System”	means: (a) those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources); and (c) for the avoidance of doubt includes the Development Environment;
“Security Requirements”	mean the security requirements in Annex 1 to this Schedule [♦] (<i>Security Management</i>);
“Supplier Personnel”	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Contract;
“Support Location”	means a place or facility where or from which individuals may access or Handle the Code or the Buyer Data;
“Support Register”	means the register of all hardware and software used to provide the Services produced and maintained for Higher Risk Contracts in accordance with Paragraph 12 of the Security Requirements;
“Third-party Software Module”	means any module, library or framework that: (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 Buyer 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  (*Security Management*) sets out:

- (a) the assessment of this Contract as either a:
 - (i) higher risk agreement; or
 - (ii) standard agreement,
 in Paragraph 0;
- (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 Buyer Data;
 - (iv) the Services; and
 - (v) the Supplier Information Management System;
- (c) the principle of co-operation between the Supplier and the Buyer on security matters, in Paragraph 5;
- (d) the Buyer's access to the Supplier Personnel and Supplier Information Management System, in Paragraph 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 Buyer 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 Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors;
- (b) the security and integrity of the Developed System; and
- (c) the security of the Supplier Information Management System.

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

6 Security Requirements

6.1 The Supplier shall:

- (a) comply with the Security Requirements; and
- (b) 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 Sub-contractor; 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 [x] (*Security Management*) 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 Personnel

7.1 The Supplier must ensure that it all times it maintains within the Supplier Personnel sufficient numbers of qualified, skilled security professionals to ensure the Supplier complies with the requirements of this Schedule 5 (*Security Management*).

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 5 (*Security Management*); 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 Personnel and treated for the purposes of this Contract as Key Personnel, 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 Personnel 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 Personnel, including, for the avoidance of doubt, the Sub-contractor Personnel;
- (b) access to the Supplier Information Management System, including those parts of the Supplier Information Management System under the control of, or operated by, any Sub-contractor; and
- (c) such other information and/or documentation that the Buyer or its authorised representatives may require,

to allow the Buyer to audit the Supplier and its Sub-contractors' compliance with this Schedule [] (*Security Management*) 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 Buyer 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 Buyer Data that is classified as OFFICIAL; and
 - (b) is not intended for the Handling of Buyer 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 Buyer Data; and
 - (b) if it becomes aware that any Buyer 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 Buyer Data.
- 9.3 The Supplier must, and must ensure that Sub-contractors and Supplier Personnel, when Handling Buyer 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 [] (*Security Management*) the provisions of this Schedule [] (*Security Management*) 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 higher-risk agreement.

Preparation of Security Management Plan

- 11.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule [◆] (*Security Management*) and the Contract in order to ensure the security of the Development Environment, the Developed System, the Buyer 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 [◆] (*Security Management*), including the Security Requirements;
 - (b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Development Environment, the Developed System, the Buyer Data, the Buyer, the Services and/or users of the Services; and
 - (c) the following information, so far as is applicable, in respect of each Sub-contractor:
 - (i) the Sub-contractor's:
 - (A) legal name;
 - (B) trading name (if any);
 - (C) registration details (where the Sub-contractor is not an individual);
 - (ii) the Relevant Certifications held by the Sub-contractor;
 - (iii) the Sites used by the Sub-contractor;
 - (iv) the Development Activity undertaken by the Sub-contractor;
 - (v) the access the Sub-contractor has to the Development Environment;
 - (vi) the Buyer Data Handled by the Sub-contractor;
 - (vii) the Handling that the Sub-contractor will undertake in respect of the Buyer Data;
 - (viii) the measures the Sub-contractor has in place to comply with the requirements of this Schedule [◆] (*Security Management*);
 - (d) the Register of Support Locations and Third-party Tools;
 - (e) the Modules Register;
 - (f) the Support Register;
 - (g) details of the steps taken to comply with:
 - (i) the Secure Development Guidance; and

- (ii) the secure development policy required by the ISO/IEC 27001:2022 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 Buyer 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 [] (Security Management), 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 [] (Security Management):

- (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 [] (*Security Management*);
- (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 5 (*Security Management*); 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 [] (*Security Management*)):
 - (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 Buyer Data and, as a consequence, the performance by the Supplier of its obligations under this Schedule [] (*Security Management*); 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 Sub-contractors, at all times:
- (a) undertake the Development Activity;
 - (b) host the Development Environment; and
 - (c) store, access or Handle Buyer 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 as onerous as those relating to Sub-contractors in this Schedule 5 (*Security Management*);
 - (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
 - (d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity’s compliance with the binding agreement; and
 - (e) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.
- 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 Buyer Data at that location or those locations;
 - (ii) sanitise, in accordance with instructions from the Buyer, such equipment within the information and communications technology system used to store, access or Handle Buyer 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 5 (*Security Management*);
 - (c) the Supplier or Sub-contractor has taken reasonable steps to assure itself that the entity complies with the binding agreement;
 - (d) the Supplier has provided the Buyer with such information as the Buyer requires concerning:
 - (i) the entity;
 - (ii) the arrangements with the entity; and
 - (iii) the entity's compliance with the binding agreement; and
 - (e) the Buyer has not given the Supplier a Prohibition Notice under Paragraph 1.11.

Third-party Tools

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

- (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 [x] (Security Management);
- (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 Sub-contractors 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 Sub-contractors 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 Buyer Data;
- (b) the operator of the Secure Location has prepared a physical security risk assessment and a site security plan for the Secure Location; and
- (c) 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 Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel in:
- (a) Development Activity;

- (b) any activity that provides access to the Development Environment; or
 - (c) any activity relating to the performance and management of the Services
- unless:
- (d) that individual has passed the security checks listed in Paragraph 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 Personnel 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 Personnel, it must:

- (a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
- (b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor Personnel will perform as the Buyer reasonably requires; and
- (c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

Annual training

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

- (a) General training concerning security and data handling; and
- (b) Phishing, including the dangers from ransomware and other malware; and
- (c) the Secure by Design Principles.

Staff access

- 3.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
- 3.6 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
- 3.7 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data, or part of that Buyer Data specified by the Buyer, as soon as practicable and in any event within 24 hours of the request.

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 Personnel 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 Personnel undertake Remote Working only in accordance with the Remote Working Policy;
 - (d) may not permit any Supplier Personnel 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 Personnel from printing documents in any Remote Location;
 - (b) restricting or prohibiting Supplier Personnel from downloading any Buyer 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 Personnel 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 Personnel subject to the proposed Remote Working Policy:
 - (i) the types and volumes of Buyer Data that the Supplier Personnel can Handle in a Remote Location and the Handling that those Supplier Personnel 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 Sub-contractor (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 Personnel must comply; and
- (f) how the Supplier or the Subcontractor (as applicable) will:
 - (i) communicate the Remote Working Policy and business rules to Supplier Personnel; 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 Buyer 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 Buyer Data or Code must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

- (b) users must authenticate before gaining access;
- (c) all Buyer Data and Code must be encrypted using a encryption tool agreed to by the Buyer;
- (d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
- (e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data and Code to ensure the security of that Buyer Data and Code;
- (f) the Supplier or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data or Code stored on the device and prevent any user or group of users from accessing the device;
- (g) all End-user Devices are within the scope of any Relevant Certification.

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 [] (*Security Management*) 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 Buyer Data:

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

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 cyber-attack 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 non-automated methods both as part of:
 - (A) any original coding; and

(B) at any time the Code is changed;

- (c) ensure that all Development Environments:
 - (i) protect access credentials and secret keys;
 - (ii) 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 cloud-based code repository that has been assessed against the NCSC Cloud Security Principles;
- 7.2 ensure user access to code repositories is authenticated using credentials, with passwords or private keys;
- 7.3 ensure secret credentials are separated from source code.
- 7.4 run automatic security testing as part of any deployment of the Developed System.

8 Development and Testing Data

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 Buyer Data where the licence terms of that software purport to grant the licensor rights to Handle the Buyer Data greater than those rights strictly necessary for the use of the software.

11 Third-party Software Modules

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

- 11.2 Where the Supplier or a Sub-contractor incorporates a Third-party Software Module into the Code, the Supplier must:
- (a) verify the source and integrity of the Third-party Software Module by cryptographic signing or such other measure that provides the same level of assurance;
 - (b) perform adequate due diligence to determine whether there are any recognised security vulnerabilities with that Third-party Software Module;
 - (c) continue to monitor any such Third-party Software Module so as to ensure it promptly becomes aware of any newly-discovered security vulnerabilities;
 - (d) take appropriate steps to minimise the effect of any such security vulnerability on the Developed System.
- 11.3 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 higher-risk 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 Buyer Data, the Supplier must agree with the Buyer the encryption methods that it and any Sub-contractors that Handle Buyer Data will use to comply with this Paragraph 13.

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

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

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

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

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

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

- (a) immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
- (b) provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
- (c) provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.

13.7 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to

Error! Reference source not found.

agree appropriate protective measures for the unencrypted Buyer Data.

13.8 Where the Buyer and Supplier reach agreement, the Supplier must document:

- (a) the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
- (b) the protective measure that the Supplier and/or Sub-contractor will put in place in respect of the unencrypted Buyer Data.

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

14 Backup and recovery of Buyer Data

Backups and recovery of Buyer Data

14.1 The Supplier must backup and recover the Buyer 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 [x] (Security Management) 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 [insert period]; and
 - (ii) a recovery point objective of [insert period]; and
- (b) a retention period of [insert period].

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 Buyer 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 Sub-contractor's System;
- (b) there is sufficient storage volume for the amount of Buyer Data to be backed up;
- (c) all back-up media for Buyer Data is used in accordance with the manufacturer's usage recommendations;
- (d) newer backups of Buyer 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 Buyer Data to:
 - (i) identifies any backup failure; and

- (ii) confirm the integrity of the Buyer Data backed up;
- (f) any backup failure is remedied promptly;

- (g) the backup system monitors the recovery of Buyer Data to:
 - (i) identify any recovery failure;
 - (ii) confirm the integrity of Buyer 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/set-up-government-email-services-securely>; or
 - (ii) the NCSC (current version at <https://www.ncsc.gov.uk/collection/email-security-and-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 Buyer 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 Sub-contractor applies security patches to any vulnerabilities in the Supplier Information Management System no later than:

- (a) seven (7) days after the public release of patches for vulnerabilities classified as “critical”;
- (b) thirty (30) days after the public release of patches for vulnerabilities classified as “important”; and
- (c) sixty (60) days after the public release of patches for vulnerabilities classified as “other”.

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 [Contract Year]; and
- (c) when required to do so by the Buyer;

undertake the following activities:

- (d) conduct security testing of the Supplier Information Management System, insofar as it relates to the Developed System but excluding the Development Environment (an “**IT Health Check**”) in accordance with Paragraph 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 Buyer Data or that are Privileged Users;
 - (c) allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
 - (d) maintain records detailing each person's access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
- 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 Buyer Data and the Code to:

- (a) identify and prevent potential Breaches of Security;
- (b) respond effectively and in a timely manner to Breaches of Security that do occur;
- (c) identify and implement changes to the Supplier Information Management System to prevent future Breaches of Security; and
- (d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier Information Management System or the Developed System

(the “**Protective Monitoring System**”).

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 Buyer Data;
- (c) the detection and prevention of any attack on the Supplier Information Management System or the Development Environment using common cyber-attack techniques;
- (d) any other matters required by the Security Management Plan.

Event logs

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 [] (*Security Management*) and the Data Protection Laws as they apply to Buyer Data;
- (b) inspect the Supplier Information Management System (or any part of it);
- (c) review the integrity, confidentiality and security of the Buyer Data; and/or
- (d) review the integrity and security of the Code.

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 Buyer Data;
- (b) there has been or is likely to be a Security Breach affecting the Buyer Data or the Code; or
- (c) where vulnerabilities, or potential vulnerabilities, in the Code have been identified by:
 - (i) an IT Health Check; or
 - (ii) a Breach of Security.

Conduct of audits

- 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 Supplier Information Management System the Buyer considers reasonable having regard to the purpose of the audit; and
- (b) use reasonable endeavours to ensure that the conduct of the audit does not unreasonably disrupt the Supplier or Sub-contractor (as applicable) or delay the provision of the Services.

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

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

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 Buyer 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 Buyer 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 Buyer Data

24.1 The Supplier must create and maintain a register of:

- (a) all Buyer Data the Supplier, or any Sub-contractor, receives from or creates for the Buyer; and
- (b) those parts of the Supplier Information Management System, including those parts of the Supplier Information Management System that are operated or controlled by any Sub-

contractor, on which the Buyer Data is stored,
(the “**Buyer Data Register**”).

24.2 The Supplier must:

- (a) review and update the Buyer Data Register:
 - (i) within 10 Working Days of the Supplier or any Sub-contractor changes those parts of the Supplier Information Management System on which the Buyer Data is stored;
 - (ii) within 10 Working Days of a significant change in the volume, nature or overall sensitivity of the Buyer Data stored on the Supplier Information Management System;
 - (iii) at least once every 12 (twelve) months; and
- (b) provide the Buyer with a copy of the Buyer Data Register:
 - (i) whenever it updates the Buyer Data Register; and
 - (ii) otherwise when the Buyer requests.

24.3 Subject to Paragraph 24.4, the Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

- (a) when requested to do so by the Buyer; and
- (b) using a deletion method agreed with the Buyer that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

24.4 Paragraph 24.4 does not apply to Buyer 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 Buyer Data held by the Supplier or Sub-contractor, including any or all Code:

- (a) when requested to do so by the Buyer; and
- (b) using the method specified by the Buyer.

Annex 2 Security Management Plan Template

[Insert EITHER Security Management Plan template OR link to Guidance including Security Management Plan template]

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

[To be used only where the Buyer has selected the relevant option in Paragraph 0]

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	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 significance	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
<p>Source secure technology products</p> <p>Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.</p>	associated with the product and are subject to agreement with the Buyer.	
	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 third-party 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.	
<p>Principle 3</p> <p>Adopt a risk-driven approach</p> <p>Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape.</p>	As provided by the Buyer, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	
	The Supplier supports the Buyer with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	
	<p>The Supplier supports the Buyer with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions.</p> <p>During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is</p>	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
	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.	
Principle 5 Build in detect and respond security Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring,	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.	
	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
alerting and response capabilities. These must be continually tested and iterated.	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.	
Principle 7 Minimise the attack surface Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use.	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.	
	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.	

Secure by Design Principle	Requirements	How the Supplier will meet the requirement
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.	
	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	The Supplier responsible for building the digital service works with the Buyer to assess the security impact of	

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

Crown Copyright 2021

Secure by Design Principle	Requirements	How the Supplier will
Make changes securely Embed security into the design, development and deployment processes to ensure that the security impact of changes is considered alongside other factors.	changes before these are made to digital services and infrastructure.	
	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.	