DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	**C355896**
THE BUYER:	**NHS England**
BUYER ADDRESS	**7-8 Wellington Place, Leeds, LS1 4AP**
THE SUPPLIER:	**IBM United Kingdom Limited**
SUPPLIER ADDRESS:	**Building C IBM Hursley office, Hursley Park Road, Winchester, Hampshire, United Kingdom, SO21 2JN**
REGISTRATION NUMBER:	**14089257**
DUNS NUMBER:	**210151718**

DPS SUPPLIER REGISTRATION SERVICE ID: **N/A**

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 19th June 2025

It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORIES:
Non-assured NCSC Services, Security Operations Centre (SOC), Cyber Essentials Plus, Clearance: Security Check, Networks, Cloud, Endpoint/applications, Government, Health, Critical National Infrastructure.

ORDER INCORPORATED TERMS

The following documents are incorporated into this Order 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 Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM3764iii
        - 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 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

    - Order Schedules for RM3764iii
        - Order Schedule 1 (Transparency Reports)
        - Order Schedule 4 (Order Tender)
        - Order Schedule 5 (Pricing Details)
        - Order Schedule 6 (ICT Services)
        - Order Schedule 7 (Key Supplier Staff)
        - Order Schedule 8 (Business Continuity and Disaster Recovery)
        - Order Schedule 9 (Security) Part B
        - Order Schedule 10 (Exit Management)
        - Order Schedule 15 (Order Contract Management)
        - Order Schedule 18 (Background Checks)
        - Order Schedule 20 (Order Specification)
        - Order Schedule 22 (Secret Matters)
4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6-Not used

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

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:
None

The Core Terms shall be amended with deletions scored-through and insertions underlined as follows:

Special Term 1: Clause 3 (What needs to be delivered)

The following wording shall be included as **new Clauses 3.4, 3.5 and 3.6** of the Core Terms, and references to these clauses shall also be added to clause 10.5.7:

"3.4 The Supplier warrants and represents that it shall comply throughout the term with the data security and protection toolkit (DSP Toolkit), an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards and supports key requirements of the GDPR, which can be accessed from https://www.dsptoolkit.nhs.uk/, as may be amended or replaced by the Buyer or the Department of Health and Social Care from time to time.

3.5 The Supplier further warrants and represents that it shall comply throughout the term with:

(a) the Baseline Security Requirements (as set out in Appendix 1 of Order Schedule 9 (Security) Part B;

(b) Good Industry Practice;

(c) the Buyer's Security Policy and the ICT Policy;

(d) ISO/IEC27001 and ISO/IEC27002.

3.6 The Supplier warrants and represents that for any system, used in the provision of the Services, which holds any protectively marked Government Data it shall comply throughout the term with:

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

(b) guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets

(c) the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection

(d) 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, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

(e) the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles".

Special Term 2: Clause 9.1 Intellectual Property Rights (IPRs)

[redacted]

Special Term 3: Clause 10.3 (Ending the Contract without a reason)

Clause 10.3.2 shall be amended, and a new Clause 10.3.3 shall be inserted, as follows:

"10.3.2 Each Buyer has the right to terminate their Order Contract at any time without reason or liability by giving the Supplier not less than 30 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies. Without prejudice to Clause 10.3.3, the Buyer shall have no liability in respect of any costs incurred by the Supplier arising from such termination.

10.3.3 The Parties acknowledge and agree that:

(a) the Buyer's right to terminate under Clause 10.3.2 is reasonable in view of the subject matter of the Order Contract and the nature of the Deliverables being provided.

(b) the Order Contract Charges paid during the notice period given by the Buyer in accordance with Clause 10.3.2 are a reasonable form of compensation and are deemed to fully cover any avoidable costs or losses incurred by the Supplier which may arise (directly or indirectly) as a result of the Buyer exercising the right to terminate under Clause 10.3.2."

Special Term 4: Clause 14 (Data Protection)

The following wording shall be included as a new **Clause 14.12 (Data Protection)** of the Core Terms:

*"*14.12. Without limitation to the obligations as set out in Joint Schedule 11 (Processing Data) and the Order Form, the Supplier shall:

14.12.1 provide a draft template Data Protection Impact Assessment for the Buyer's review;

14.12.2 consider the Buyer's feedback and shall update the draft template Data Protection Impact Assessment and associated guidance notes, prior to the Start Date of the Contract;

14.12.3 provide a further draft Data Protection Impact Assessment as a part of the Order Procedure for each Deliverable for each commission under the Contract;

14.12.4 be responsible for updating its Data Protection Impact Assessment at each material change of the Deliverables (including but not limited to each release of new software) and following any Variation."

Special Term 5: Clause 23 (Transferring responsibilities)

New clauses 23.7, 23.8 and 23.9 shall be inserted into the Core Terms, as follows:

"23.7 The Supplier may only Sub-Contract all or part of the Deliverables under the Contract with the prior written approval of the Buyer.

23.8 If the Supplier chooses to use Subcontractors, this will be detailed in any bid along with the percentage of delivery allocated to each Subcontractor.

"23.9 Notwithstanding any approval provided by the Buyer pursuant to Clause 23.7, the Supplier remains solely responsible for the provision of the Deliverables in accordance with the terms of the Contract."

Special Term 6: DPS Joint Schedule 6 (Key Subcontractors)

The following wording shall be included as a new **Paragraph 1.4.6** of DPS Joint Schedule 6 (Key Subcontractors):

"*1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:*

1.4.6 The Dun & Bradstreet Failure Rating score of the Key Subcontractor."

Special Term 7: DPS Order Schedule 9 (Security)

The following wording shall be included as a new **Part C** of DPS Order Schedule 9 (Security):

Part C: Commodity Service Security Requirements

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

["ISMS" means the information security management system and process developed by the Supplier in accordance with paragraph 2 (ISMS) as updated from time to time; and]

"**Security Management Plan**" means the Supplier's security management plan prepared pursuant to paragraph 2.

1. The Supplier will ensure that any Supplier system, used in the provision of the Services, which holds any protectively marked Government Data will comply with the principles in the Security Policy Framework at:

   - https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at https://www.gov.uk/government/publications/government-security-classifications
   - guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protection-sensitive-information-and-assets
   - the National Cyber Security Centre's (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
   - 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, available at https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
   - the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

2. If requested to do so by the Buyer, before entering into this Contract the Supplier will, within 15 Working Days of the date of this Contract, develop (and obtain the Buyer's Approval of) a Security Management Plan and an Information Security Management System. After Buyer Approval the Security Management Plan and Information Security Management System will apply during the Term of this Contract. Both plans will protect all aspects and processes associated with the delivery of the Services. This clause replaces clauses 3.1 and 4.1 of DPS Order Schedule 9 (Security).

3. The Supplier will immediately notify the Buyer of any breach of security of the Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer Confidential Information however it may be recorded.

4. Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance, available at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Special Term 8: Clause 11.5 Data Protection Indemnity

For clarity, clause 11.5 of the CCS Core Terms is amended to insert the following to align with Special Term 7 of the RM3764iii DPS Appointment Form:

In spite of Clauses 11.1, 11.2 but subject to Clauses 11.3 and 11.4, the Supplier's aggregate liability in each and any Contract Year under each Contract under Clause 14.8 shall in no event exceed £10 million.

ORDER START DATE: 19th June 2025

ORDER EXPIRY DATE: 23rd April 2028

ORDER INITIAL PERIOD: 34 Months

ORDER OPTIONAL EXTENSION 2 x 12-month options to extend

DELIVERABLES
See details in Order Schedule 20, Section 7 (Order Specification)

MAXIMUM LIABILITY
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is [redacted] Estimated Charges in the first 12 months of the Contract.

ORDER CHARGES
See details in Order Schedule 5 (Pricing Details)
Order Value Initial Period, including Surge Support: [redacted]

REIMBURSABLE EXPENSES
None. Expenses are not chargeable under this call-off contract.

PAYMENT METHOD
Monthly in arrears

BUYER'S INVOICE ADDRESS:
Invoices should be submitted via electronic invoicing Tradeshift. https://nhssbs.support.tradeshift.com or in the limited circumstances where electronic invoicing is not possible, please email invoices and credit notes to the following email address sbs.apinvoicing@nhs.net with the billing address on the invoice being:
NHS ENGLAND
X24 PAYABLES K005
PO BOX 312
LEEDS LS11 1HP

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]

[redacted]

BUYER'S ENVIRONMENTAL POLICY
NHS England Social Value Charter available online at:
https://digital.nhs.uk/about-nhs-digital/technology-suppliers/nhs-digital-social-value-charter

BUYER'S SECURITY POLICY
Appended at Order Schedule 9- Security-Annex 2

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]

SUPPLIER'S CONTRACT MANAGER
[redacted]

PROGRESS REPORT FREQUENCY
See Order Schedule 20 - Specification

PROGRESS MEETING FREQUENCY
See Order Schedule 20 - Specification

KEY STAFF
Please see Order Schedule 7- Supplier Key Staff

KEY SUBCONTRACTOR(S)
None

COMMERCIALLY SENSITIVE INFORMATION
See DPS Joint Schedule 4 – Commercially Sensitive Information

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT

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

CONTRACT SIGNATURES

For and on behalf of the Supplier:

[redacted]

Date Signed: 6th June 2025

For and on behalf of the Buyer:

[redacted]

Date Signed: 10 June 2025

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]	
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		
Reason for the variation:	**[insert** reason]	
An Impact Assessment shall be provided within:	**[insert** number] days	
Impact of Variation		
Likely impact of the proposed variation:	**[Supplier to insert** assessment of impact]	
Outcome of Variation		
Contract variation:	This Contract detailed above is varied as follows: • **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]	
Financial variation:	Original Contract Value:	£ **[insert** amount]
	Additional cost due to variation:	£ **[insert** amount]
	New Contract value:	£ **[insert** amount]

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Joint Schedule 3 (Insurance Requirements)

1. The insurance you need 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 an Order 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 DPS 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 Order 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 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 you aren't 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 you must provide

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. Making sure you are insured to the required amount

5.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

6. Cancelled Insurance

6.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

6.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in

dealing with such claims including without limitation providing information and documentation in a timely manner.

7.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

7.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

7.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.

ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the DPS 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 [redacted];

1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than [redacted]; and

1.3 employer's liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than [redacted].

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.	Date	Item(s)	Duration of Confidentiality
1	16th April 2025	All pricing information or financial modelling set out in the tender response and / or Call-Off Schedule 5 (Pricing Details) including any changes from Change Control.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
2	16th April 2025	All information relating to the Open Book Data, any financial reports and the exercise of the Authority's audit rights.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
3	16th April 2025	All information relating to the financial standing of the Supplier (that is not otherwise in the public domain), and the occurrence and/or consequences of any Financial Distress Events.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
4	16th April 2025	All information identifying third parties and which is subject to an obligation of confidentiality to that third party including, but not limited to credentials and references for work for other clients.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
5	16th April 2025	Call-Off Schedule 4 (Supplier Solution) and related processes, organisation, and technology as set out in the tender response.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.

No.	Date	Item(s)	Duration of Confidentiality
6	16th April 2025	All Personal Data, and all other information relating to individuals including, but not limited to, CVs, biographies, pen portraits, contact details, and Key Supplier Staff named in Call-Off Schedule 7 (Supplier Key Staff).	Indefinitely
7	16th April 2025	All information relating to Supplier's business plans, strategy, competitive position, approach, and methodologies.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
8	16th April 2025	Supplier IPRs, Third Party IPRs, and any modifications and/or enhancements to these.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
9	16th April 2025	All information relating to Supplier's insurance arrangements and accounts that have not been subject to public reporting.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
10	16th April 2025	The Supplier's Security Management Plan set out in Call-Off Schedule 9.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.

No.	Date	Item(s)	Duration of Confidentiality
11	16th April 2025	Records of Governance as detailed in Call-Off Schedule 15 in so far as these detail Pricing, breakdown of Costs, financial information, Charges discussions, in connection with Contract Change Authorisation Notices, Impact Assessments, Impact Assessment Estimates, presentation materials and/or models.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
12	16th April 2025	The Supplier's Rectification Plans.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.
13	16th April 2025	The Supplier's Business Continuity and Disaster Recovery Plan.	For the duration of the Buyer Contract Term and for a period of seven (7) years thereafter.

Joint Schedule 6 (Key Subcontractors)

1. Restrictions on certain subcontractors

1.1 The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.

1.2 The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform 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 CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a New Key Subcontractor then they will be added to the Platform. 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. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

1.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

1.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

1.3.3 the proposed Key Subcontractor employs unfit persons.

1.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

1.4.1 the proposed Key Subcontractor's name, registered office and company registration number;

1.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

1.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm's-length" terms;

1.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;

1.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and

1.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:

1.5.1 a copy of the proposed Key Sub-Contract; and

1.5.2 any further information reasonably requested by CCS and/or the Buyer.

1.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

1.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

1.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

1.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

1.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

1.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the DPS 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 (What happens if the contract ends) of this Contract; and

1.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key 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"	the minimum credit rating level for the Monitored Company as set out in the third Column of the table at Annex 2 and
"Financial Distress Event"	the occurrence or one or more of the following events: a) the credit rating of the Monitored Company dropping below the applicable Credit Rating Threshold; b) the Monitored Company issuing a profits warning to a stock exchange or making any other public announcement about a material deterioration in its financial position or prospects; c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Monitored Party; d) Monitored Company committing a material breach of covenant to its lenders; e) a Key Subcontractor (where applicable) notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute; or f) any of the following: i) commencement of any litigation against the Monitored Company with respect to financial indebtedness or obligations under a contract; ii) non-payment by the Monitored Company of any financial indebtedness;

	iii) any financial indebtedness of the Monitored Company becoming due as a result of an event of default; or iv) the cancellation or suspension of any financial indebtedness in respect of the Monitored Company in each case which CCS reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance of any Contract and delivery of the Deliverables in accordance with any Order Contract;
"Financial Distress Service Continuity Plan"	a plan setting out how the Supplier will ensure the continued performance and delivery of the Deliverables in accordance with each Order Contract in the event that a Financial Distress Event occurs;
"Monitored Company"	Supplier [the DPS Guarantor/ [and Order Guarantor] or any Key Subcontractor]
"Rating Agency"	the rating agency stated 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 termination or expiry of this 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 credit rating issued for the Monitored Companies by the Rating Agency is as set out in Annex 2.

3.2 The Supplier shall promptly (and in any event within ten (10) Working Days) notify CCS in writing if there is any downgrade in the credit rating issued by the Rating Agency for a Monitored Company which means that the credit rating for the Monitored company falls below the Credit Rating Threshold.

3.3 If there is any such downgrade credit rating issued by the Rating Agency for a Monitored Company the Supplier shall at CCS' request ensure that the Monitored Company's auditors thereafter provide CCS within 10 Working Days of the end of each Contract Year and within 10 Working Days of written request by CCS (such requests not to exceed 4 in any Contract Year) with written calculations of the quick ratio for the Monitored Company as at the end of each Contract Year or such other date as may be requested by CCS. For these purposes the "quick ratio" on any date

means:

$$\frac{A + B + C}{D}$$

where:

A	is the value at the relevant date of all cash in hand and at the bank of the Monitored Company];
B	is the value of all marketable securities held by the Supplier the Monitored Company determined using closing prices on the Working Day preceding the relevant date;
C	is the value at the relevant date of all account receivables of the Monitored]; and
D	is the value at the relevant date of the current liabilities of the Monitored Company].

3.4 The Supplier shall:

3.4.1 regularly monitor the credit ratings of each Monitored Company with the Rating Agency; and

3.4.2 promptly notify (or shall procure that its auditors promptly notify) CCS in writing following the occurrence of a Financial Distress Event or any fact, circumstance or matter which could cause a Financial Distress Event and in any event, ensure that such notification is made within 10 Working Days of the date on which the Supplier first becomes aware of the Financial Distress Event or the fact, circumstance or matter which could cause a Financial Distress Event.

3.5 For the purposes of determining whether a Financial Distress Event has occurred the credit rating of the Monitored Company shall be deemed to have dropped below the applicable Credit Rating Threshold if the Rating Agency has rated the Monitored Company at or below the applicable Credit Rating Threshold.

4. What happens if there is a financial distress event

4.1 In the event of a Financial Distress Event then, immediately upon notification of the Financial Distress Event (or if CCS becomes aware of the Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and CCS shall have the rights and remedies as set out in Paragraphs 4.3 to 4.6.

4.2 In the event that a Financial Distress Event arises due to a Key Subcontractor notifying CCS that the Supplier has not satisfied any sums properly due under a specified invoice and not subject to a genuine dispute then, CCS shall not exercise any of its rights or remedies under Paragraph 4.3 without first giving the Supplier ten (10) Working Days to:

4.2.1 rectify such late or non-payment; or

4.2.2 demonstrate to CCS's reasonable satisfaction that there is a valid reason for late or non-payment.

4.3 The Supplier shall and shall procure that the other Monitored Companies shall:

4.3.1 at the request of CCS meet CCS as soon as reasonably practicable (and in any event within three (3) Working Days of the initial notification (or awareness) of the Financial Distress Event) to review the effect of the Financial Distress Event on the continued performance of each Contract and delivery of the Deliverables in accordance each Call-Off Contract; and

4.3.2 where CCS reasonably believes (taking into account the discussions and any representations made under Paragraph 4.3.1) 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 Supplier in accordance with this Paragraph with any Buyer who has entered into a Call-Off Contract with the Supplier.

5. When CCS or the Buyer can terminate for financial distress

5.1 CCS shall be entitled to terminate this Contract and Buyers shall be entitled to terminate their Call-Off Contracts for material Default if:

5.1.1 the Supplier fails to notify CCS of a Financial Distress Event in accordance with Paragraph 3.4;

5.1.2 CCS and the Supplier fail to agree a Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraphs 4.3 to 4.5; and/or

5.1.3 the Supplier fails to comply with the terms of the Financial Distress Service Continuity Plan (or any updated Financial Distress Service Continuity Plan) in accordance with Paragraph 4.6.3.

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 Agency reviews and reports subsequently that the credit rating does 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 AGENCY

Dun & Bradstreet

ANNEX 2: CREDIT RATINGS & CREDIT RATING THRESHOLDS

Part 1: Current Rating

Entity	Credit rating (D&B Failure Rating)	Credit Rating Threshold
Supplier (IBM United Kingdom Limited)	[redacted]	

Joint Schedule 10 (Rectification Plan)

Request for [Revised] Rectification Plan			
Details of the Default:	[**Guidance:** Explain the Default, with clear schedule and clause references as appropriate]		
Deadline for receiving the [Revised] Rectification Plan:	[**add** date (minimum 10 days from request)]		
Signed by [CCS/Buyer] :		Date:	
Supplier [Revised] Rectification Plan			
Cause of the Default	[**add** cause]		
Anticipated impact assessment:	[**add** impact]		
Actual effect of Default:	[**add** effect]		
Steps to be taken to rectification:	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	
Timescale for complete Rectification of Default	[X] Working Days		
Steps taken to prevent recurrence of Default	**Steps**	**Timescale**	
	1.	[date]	
	2.	[date]	
	3.	[date]	
	4.	[date]	
	[…]	[date]	

Signed by the Supplier:		Date:	
Review of Rectification Plan [CCS/Buyer]			
Outcome of review	[Plan Accepted] [Plan Rejected] [Revised Plan Requested]		
Reasons for Rejection (if applicable)	[**add** reasons]		
Signed by [CCS/Buyer]		Date:	

Joint Schedule 11 (Processing Data)

Status of the Controller

1. 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. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where there 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

2. 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.

3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

4. 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 Services;

(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.

5. 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 promptly 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 Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(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 EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

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

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound,

uses its best endeavours to assist the Controller in meeting its obligations); and

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

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 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 Request (or purported Data Subject 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 Data Loss Event.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly 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 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 Data Loss Event; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

9. 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 GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

14. The Relevant Authority may, at any time on not less than 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).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 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

16. 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 GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

17. 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.

18. 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.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 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.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

21. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

22. 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 GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

25. 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.

26. 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).*

27. 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)*.

28. Notwithstanding the general application of paragraphs 2 to 15 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 paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data A) Template

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.

1.1 The contact details of the Relevant Authority's Data Protection Officer are: [redacted] nhsdigital.dpo@nhs.net

1.2 The contact details of the Supplier's Data Protection Officer are: [redacted]

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

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

Description	Details
Identity of Controller for each Category of Personal Data	**The Relevant Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data: The Authority, as Data Controller, is required to process Personal Data in order to deliver its statutory services. The Supplier will have access to this Personal Data in the course of providing the Services.
Duration of the Processing	For the duration of this Order Contract and Work Orders or Variations arising hereunder.
Nature and purposes of the Processing	Collection, transformation, storage, correlation and analysis of event data from systems, services and individual devices for the purpose of detection, prevention, incident handling and mitigation of cyber security threats, risks and attacks across the monitored estate, which event data, whilst not intended, may contain Personal Data.

<table>
<tr><td>Type of Personal Data</td><td>The below is between NHS England and The Supplier IBM

Name

Email Address (Work only)

Mobile Phone Number / Device Number/ IMEI No (NHS & Care Address only)

Username data for systems such as Confluence, Jira.</td></tr>
<tr><td>Categories of Data Subject</td><td>This will depend on the nature of the product/systems/ services being utilised during the delivery of services under the contract but could include, but not limited to,

Customer, Supplier, Citizen.</td></tr>
<tr><td>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</td><td>All relevant data to be deleted after the expiry or termination of this Order Contract unless longer retention is required by Law or the terms of any Work Order arising hereunder.</td></tr>
<tr><td>Sub Processors</td><td>IBM Services Centre UK Limited</td></tr>
<tr><td>Technical and Organisational Measures (TOMs)</td><td>The technical and organisational measures (TOMs) applicable to the services are described below:

<table>
<tr><th>Type</th><th>TOM #</th><th>Description</th></tr>
<tr><td>Document Management</td><td>1.1.1</td><td>Keep approval records of data security & privacy (DS&P) documents and make available for report/audit purpose.</td></tr>
</table>
</td></tr>
</table>

		Document Management	1.1.2	Create and review DS&P documents in a timely manner and review on a periodic basis	
		Document Management	1.1.3	Store and archive project related documentation in secure repository	
		Contract and Subprocessor Management	1.2.1	Create and maintain project DS&P documents that reflect the requirements of the TOMs documented in the appropriate contractual document	
		Contract and Subprocessor Management	1.2.2	Assess the impact of contract changes on the Processing of Authority Personal Data and update DS&P documentation as appropriate	
		Contract and Subprocessor Management	1.2.3	Undertake pre-screening assessments and have project personnel sign NDAs as appropriate	
		Contract and Subprocessor Management	1.2.4	Enter into written agreements with all Subprocessors to impose on them substantially similar obligations as are set out in the appropriate contractual document, in particular providing sufficient guarantees to implement appropriate technical and organizational measures	
		Contract and Subprocessor Management	1.2.6	Monitor and document adherence to the TOMs defined in the appropriate contractual document	
		Reviews, Assessments & Audits	1.3.1	Regularly assess project risks related to processing of Personal Data	
		Reviews, Assessments & Audits	1.3.2	Implement the three lines of defence model where activities are performed to address each line of defence as appropriate based on risks by various test and audit functions	
		Reviews, Assessments & Audits	1.3.3	Follow up action plans resulting from security audits, tests and assessments	

		Risk Management and Incident Management	1.4.3	Implement an incident management process to ensure immediate reporting, impact analysis and effective corrective (and preventive) actions	
		Risk Management and Incident Management	1.4.4	Implement an effective emergency plan ensuring adequate involvement of IBM Legal in security incidents	
		Risk Management and Incident Management	1.4.5	Implement procedures for threat prevention for minimising the risk of security breaches	
		Project Management and People Management	1.5.2	Ensure Personal Data is only processed as agreed in the appropriate contractual document	
		Information Classification Scheme, Inventory and Data Map	1.6.1	Create and maintain an inventory of Authority Personal Data and security related items	
		Training	1.7.2	Conduct periodic contract specific DS&P training for Subprocessors	
		Training	1.7.3	Conduct periodic organisational level DS&P training	
		Network and Firewalls, System Logging & Monitoring and Separation of Environments	3.2.3	Manage access to and through the IBM network in a secure manner	
		Data Protection Techniques (Encryption, Psuedonymisation, Anonymisation)	3.4.1	Employ the use of encryption, pseudonymisation and/or anonymisation of Authority Personal Data in data processing activities where applicable	
		Physical Equipment and Media Handling	3.5.2	Implement security controls for workstations that process Authority Personal Data	
		Physical Equipment and Media Handling	3.5.3	Implement controls for mobile computing and communication	

				infrastructure in accordance with IBM security policies
		Physical Equipment and Media Handling	3.5.4	Securely destroy sensitive information and licensed software prior to reuse or disposal of equipment

B) DPS Contract Personal Data Processing – Not Used

Annex 2 - Joint Controller Agreement-Not Used

Order Schedule 1 (Transparency Reports)

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-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.

2. Without prejudice to the Supplier's reporting requirements set out in the DPS 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.

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.

4. The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
Performance	Actuals against Service Levels	See call-off Schedule 20 – Specification – written format and at meetings	See call-off Schedule 20 – Specification
Order Contract Charges	Breakdown of actual costs	Monthly invoices and as	Monthly in arrears
Key Subcontractors	List of any sub-contractors on this contract	Written format	As required
Social Value KPI	Report on progress against the Social Value commitment made	Written format	Quarterly
Performance management	Measures taken to improve any performanc e issues	See call-off Schedule 20 – Specification – written format and at meetings	See call-off Schedule 20 – Specification

Order Schedule 4 (Order Tender)

Tender Response

Q1-Technical merit and Approach to delivering the SOC protective monitoring

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

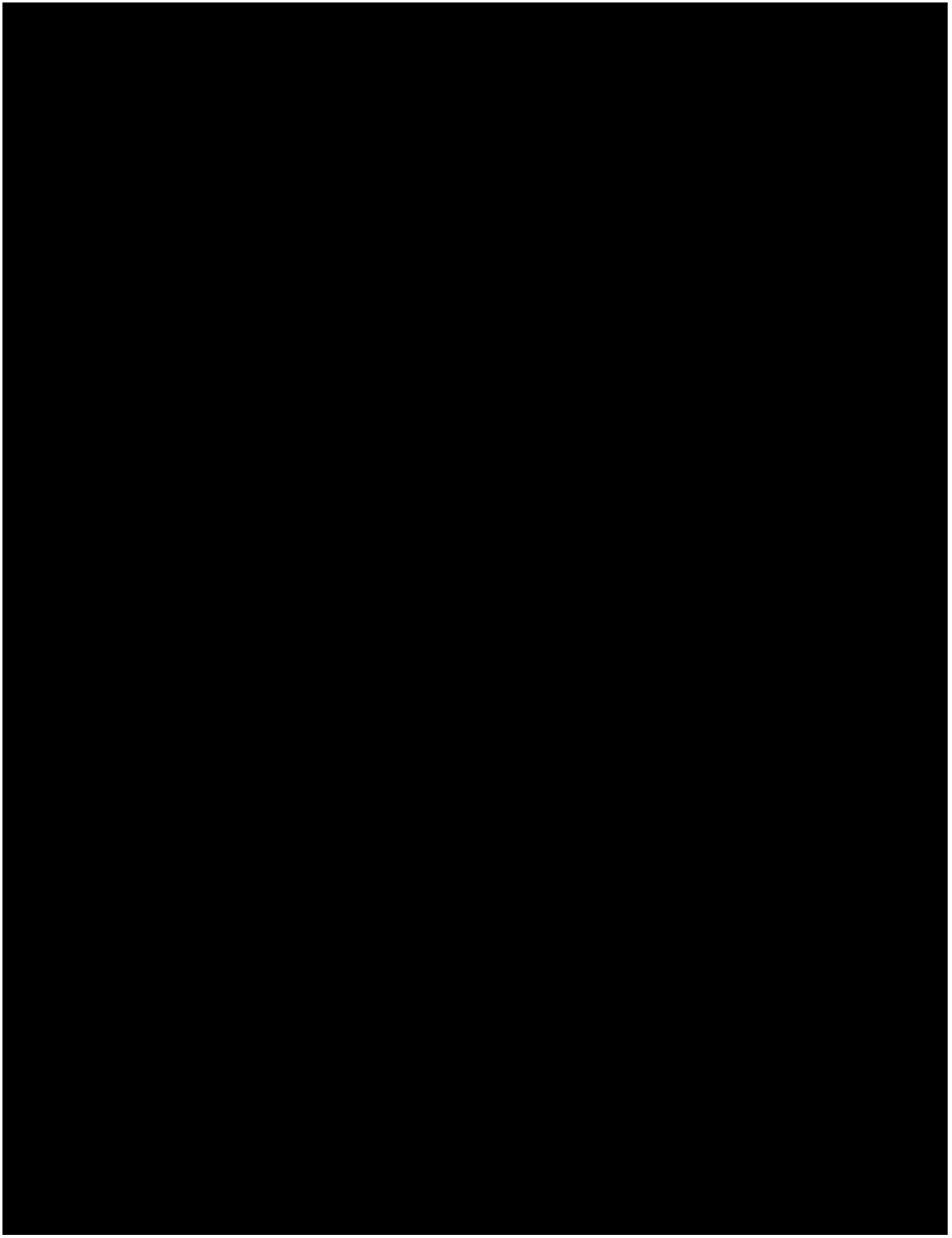
[redacted]

[redacted]

[redacted]

[redacted]

[redacted]



[redacted]

[redacted]

[redacted]

Order Schedule 5 (Pricing Details)

The below rate card is the maximum price that will apply to deliverable and services under this contract

All pricing is exclusive of VAT		
Provide the maximum rate card price for each of the Profiles. - **PLEASE NOTE - THE ROLE EXPERIENCE AND SKILL MUST MATCH THE DETAILED PROFILE PROVIDED IN APPENDIX B3, B4 and B5, FOR OTHER ROLES, SKILLS/EXPERIENCE SHOULD BE ALIGNED TO INDUSTRY STANDARD ROLES.**		
Skill/Role		**Day Rate**
[redacted]	Price: £	[redacted]
	Price: £	
	Price: £	
	Price: £	
	Price: £	
	Price: £	
	Price: £	

The below is the cost to deliver BAU and surge support services under this contract for the estimated hours per year

All pricing should be exclusive of VAT			
Provide your total fixed cost to deliver the BAU elements of this contract (not including surge costs or scalability). This should be costed up based on the day rates provided.			
[redacted]		Total Cost per annum	Total Cost over the life of the Contract
	Price: £	[redacted]	
	Hourly Rate which aligns to the Day Rate Card	**Estimate Number of Hours per year**	**Total Surge Cost Per Year**
	[redacted]		
		Total per year	
		Estimated Cost for Surge Support over the life of the Contract	
		TOTAL TO BE EVALUATED	

Please complete table below to support the BAU Total Cost above

High-level breakdown of the resource profile, per annum		**Total Cost per annum**	**Total Cost over the life of the Contract**
[redacted]	Price: £	[redacted]	
	Price: £		
	Price: £		
	Price: £		
	Price: £		
	Price: £		
	Price: £		

The below is the invoicing schedule for Mobilisation, BAU and surge support services under this contract. Charges will be invoiced in accordance with the Order Form and Clause 4 of the Core Terms.

The first and final months of each Contract Year are partial months, therefore the monthly invoice has been pro-rated accordingly.

Surge support will be invoiced in arrears on a time and materials basis, based on when services are performed. The invoicing profile shown below is pro-rated across the contract term and is provided for illustrative purposes.

[redacted]

Charges and Rate Card will be fixed for the first 3 years and will be reviewed on the anniversary of the initial term for any approved extension period thereafter. Any agreed increase will be based on RPI as set by the Office of National Statistics

(ONS), for the month of the anniversary of the execution of the contract but capped at a maximum of 3.9%.

Order Schedule 6 (ICT Services)

1. Definitions

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

"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 Order Contract which is owned by or licensed to the Buyer by a third party and which interfaces with the Supplier System or which is necessary for the Buyer to receive the Deliverables;
"Commercial off the shelf Software" or "COTS Software"	non-customised software where the IPR may be owned and licensed either by the Supplier or a third party depending on the context, and which is commercially available for purchase and subject to standard licence terms;
"Defect"	any of the following: a) any error, damage or defect in the manufacturing of a Deliverable; or b) any error or failure of code within the Software which causes a Deliverable to malfunction or to produce unintelligible or incorrect results; or c) any failure of any Deliverable to provide the performance, features and functionality specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract; or d) any failure of any Deliverable to operate in conjunction with or interface with any other Deliverable in order to provide the performance, features and functionality

	specified in the requirements of the Buyer or the Documentation (including any adverse effect on response times) regardless of whether or not it prevents the relevant Deliverable from passing any Test required under this Order Contract;
"ICT Environment"	the Buyer System and the Supplier System;
"Licensed Software"	all and any Software licensed by or through the Supplier, its Sub-Contractors or any third party to the Buyer for the purposes of or pursuant to this Order Contract, including any COTS Software;
"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;
"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 Order Schedule shall also include any premises from,

	to or at which physical interface with the Buyer System takes place;
"Software"	Specially Written Software, COTS Software and non-COTS Supplier and third party Software;
"Software Supporting Materials"	has the meaning given to it in paragraph 8.1 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 necessary to facilitate the provision of ICT services which are part of the Deliverables.

3. Buyer due diligence requirements

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

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

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

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

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

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

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

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.

4. 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 Order 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 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 any interface requirements of the Buyer specified in this Order Contract 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 Order 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, where specified by the Buyer as part of their Order Procedure, and in accordance with agreed timescales, develop 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 Order Contract Period:

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

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

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

7. ICT Audit

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

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

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

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

8. Intellectual Property Rights in ICT

8.1. **Assignments granted by the Supplier: Specially Written Software**

8.1.1. 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:

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

8.1.1.2. 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**").

8.1.2. The Supplier shall:

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

8.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan,

achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and

8.1.2.3. without prejudice to paragraph 8.1.2.2, 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.

8.1.3. 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.

8.2. **Licences for non-COTS IPR from the Supplier and third parties to the Buyer**

8.2.1. 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

8.2.2. 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 Order Contract Period and after expiry of the Order Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.

8.2.3. 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 8.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:

8.2.3.1. 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

8.2.3.2. only use such third party IPR as referred to at paragraph 8.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.

8.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 8.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.

8.2.5. The Supplier may terminate a licence granted under paragraph 8.2.1 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.

8.3. **Licenses for COTS Software by the Supplier and third parties to the Buyer**

8.3.1. 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.

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

8.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 8.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.

8.3.4. 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:

8.3.4.1. will no longer be maintained or supported by the developer; or

8.3.4.2. will no longer be made commercially available

8.4. **Buyer's right to assign/novate licences**

8.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 8.2 (to:

8.4.1.1. a Central Government Body; or

8.4.1.2. 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.

8.4.2. 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 8.2.

8.5. **Licence granted by the Buyer**

8.5.1. The Buyer grants to the Supplier a licence to use the Specially Written Software i) during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and ii) after the Contract period on the terms set out in the Open Government Licence.

8.5.2. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer 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).

8.6. **Open Source Publication**

8.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 8.6.3) 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:

8.6.1.1. suitable for publication by the Buyer as Open Source; and

8.6.1.2. based on Open Standards (where applicable),

and the Buyer may, at its sole discretion, publish the same as Open Source.

8.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:

8.6.2.1. 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;

8.6.2.2. 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;

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

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

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

8.6.2.6. do not contain any Malicious Software.

8.6.3. 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:

8.6.3.1. 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

8.6.3.2. 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. Supplier-Furnished Terms

9.1. Software Licence Terms

9.1.1.1. Terms for licensing of non-COTS third party software in accordance with Paragraph 8.2.3 are detailed in Annex A of this Order Schedule 6.

9.1.1.2. Terms for licensing of COTS software in accordance with Paragraph 8.3 are detailed in Annex B of this Order Schedule 6.

ANNEX A-Not Used

Non-COTS Third Party Software Licensing Terms

ANNEX B- Not used

COTS Licensing Terms

Order Schedule 7 (Key Supplier Staff)

1. The Annex 1 to this Schedule 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.

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

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.

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

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

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

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

5. The Supplier shall:

   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);

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

   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 2 Months' notice;

   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; and

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.

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.

Annex 1- Key Roles

Key Role	Key Staff	Contact Details
[redacted]		

Order Schedule 8 (Business Continuity and Disaster Recovery)

1. BCDR PLAN

1.1 At the Supplier's request, the Customer shall provide the Supplier with a copy of its Business Continuity & Disaster Recovery ("BCDR") Plan.

1.2 The Supplier shall develop a BCDR Plan and ensure that it is linked and integrated with the Buyer's BCDR Plan and the Supplier shall review and amend its BCDR Plan on a regular basis and as soon as is reasonably practicable on receipt of an amended Buyer BCDR Plan from the Buyer.

1.3 The Supplier shall ensure that its Sub-Contractor's BCDR Plans are integrated with the Supplier's BCDR Plan.

1.4 If there is a Disaster, the Parties shall, where applicable, implement their respective BCDR Plans and use all reasonable endeavours to re-establish their capacity to fully perform their obligations under this Order Contract. A Disaster will only relieve a Party of its obligations to the extent it constitutes a Force Majeure Event in accordance with Clause 20 (Circumstances Beyond Your Control).

Order Schedule 9 (Security)

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):

"Breach of Security"	means the occurrence of: a) 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 b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such 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 plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

2.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS 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 [redacted] security representative of the Buyer

2.3.2 [redacted] security representative of the Supplier

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.

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 an Order Procedure 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;

(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 immediately 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 3.1 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

4.3 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;

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 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;

5.1.5 any new perceived or changed security threats; and

5.1.6 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 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.

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-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 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 3.4.5;

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 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 UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG 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 (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 CESG 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 CESG, 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 and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents) 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.

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

NHS England Security Policy

NHS England Security Policy.pdf

Order Schedule 10 (Exit Management)

1. Within 20 (twenty) working days of the Start Date the Supplier must provide for the Buyer's Approval an exit plan which ensures continuity of service and which the Supplier will follow at the end of the Order Contract. The Buyer shall not unreasonably withhold Approval of the draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it

2. The Supplier must ensure that the exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the Order Contract ends before the scheduled expiry.

3. The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:

- the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- the strategy for export and migration of Buyer data from any relevant Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer
- the transfer of New IPR items to the Buyer or a Replacement Supplier
- the testing and assurance strategy for exported Buyer data
- if relevant, TUPE-related activity to comply with the TUPE regulations
- any other activities and information which are reasonably required to ensure continuity of service during the exit period and an orderly transition to the Buyer or a Replacement Supplier.

Order Schedule 15 (Order 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 5.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

3.1 The Supplier's Contract Manager 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 the delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

3.1.3 able to cancel any delegation and recommence the position himself; and

3.1.4 replaced only after the Buyer has received notification of the proposed change.

3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

3.3 Receipt of communication from the Supplier's Contract Manager by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Contract Risk Management

4.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.

4.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

4.2.1 the identification and management of risks;

4.2.2 the identification and management of issues; and

4.2.3 monitoring and controlling project plans.

4.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

4.4 The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

5. ROLE OF THE OPERATIONAL BOARD

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

No additional contract boards apply at this stage of contract award, if future boards required then this will be managed by a variation to the contract.

Order Schedule 18 (Background Checks)

See staff clearances listed in Order Schedule 20 - Specification

Order Schedule 20 (Order Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

NHS England CSOC – 24/7 Protective Monitoring

Appendix B2 - Statement of Requirements

Purpose

1.1. The Authority's Cyber Security Operation Centre has a team of analysts working in 'core hours' only (which are 9am to 5pm Monday to Friday, excluding public holidays. Under the legal direction of the Secretary of State, NHS England's CSOC is mandated to provide cyber services to the Health and Social Care (H&SC) System including full 24x7 coverage of the systems onboarded to the CSOCs monitoring. Therefore, the successful Supplier shall provide resource for 24x7 hours of coverage, to provide monitoring and security event alerting support.

2. Background to the contracting authority

2.1. Our purpose is to lead the NHS in England to deliver high-quality services for all.

2.2. We do this by ensuring that the healthcare workforce has the right numbers, skills, values and behaviours to support the delivery of excellent healthcare and health improvement to patients and the public. Read the NHS's first ever workforce plan; a once-in-a-generation opportunity to put staffing on a sustainable footing and improve patient care.

2.3. We work with the wider NHS and our partners to optimise the use of digital technology, research and innovation, and to deliver value for money and increased productivity and efficiency.

2.4. We are responsible for running the vital national IT systems which support health and social care, and the collection, analysis, publication and dissemination of data generated by health and social care services to improve outcomes for patients.

2.5. The establishment of integrated care boards within integrated care systems, which are made up of public services that provide health and care, means that NHS England is changing the way it works to best support and empower local system partners to deliver on their responsibilities.

2.6. Our NHS England Operating Framework sets out how we are supporting systems and providers to lead locally to improve the health of the population, improve the quality of patient care, tackle

inequalities and deliver care more efficiently. It describes our six longer-term aims:

1) Longer healthy life expectancy.

2) Excellent quality, safety and outcomes.

3) Excellent access and experience.

4) Equity of healthy life expectancy, quality, safety, outcomes, access and experience.

5) Value for taxpayers' money.

6) Support to society, the economy and environment.

2.7. Additional information regarding the Authority can be found on the NHS England website.

2.8. The Authority's Cyber Security Operation Centre provides critical monitoring to the National Health Service. The aim is to provide cyber awareness, cyber monitoring, threat services and incident response following the National Cyber Security Centre (NCSC) guidelines and core principles.

2.9. Under the legal direction of the Secretary of State, NHS England Cyber Operations is mandated to provide cyber services to the Health and Social Care (H&SC) System, regulated by the National Chief Information Security Officer. Internal and external capabilities are delivered through Cyber Operations including – internal, regional and national security monitoring, alerting, threat hunting and threat intelligence.

2.10. That direction requirement charges NHS England with supporting health and care organisations to be more cyber resilient and respond to incidents promptly when they happen, working with the National Cyber Security Centre. It enables NHS England to provide services and support that achieve the following security principles for the health and social care sector: to manage security risk, protect against cyber-attacks, detect cyber security incidents and minimise the impact of cyber security incidents to the system.

3. Background to requirement/ overview of requirement

3.1. The CSOC team currently work core hours of 9am to 5pm Monday to Friday, excluding public holidays. Due to the 24x7 operation of

the National Health Service, there is a requirement for full 24x7 coverage of the systems onboarded to the CSOCs monitoring which requires a third-party supplier to provide support.

3.2. In times of heightened activity there is a requirement for surge cover to ensure we are effectively monitoring the system.

4. Definitions

Expression or Acronym	Definition
BAU Service	The Supplier shall provide a Security Operations Centre service to the Authority. The Supplier shall provide “24 x 7 x 365 – Out of Hours” monitoring outside of the CSOCs core hours and the Supplier shall also provide Tier 1 Protective Monitoring support, during CSOCs core hours augmenting the Suppliers current team.
Buyer	NHS England National Cyber Security Operation Centre
Supplier	The Supplier of the 24/7 Service
Out of Hours	Any period that is not covered by the Buyers SOC team. This covered the period of 17:00 to 09:00, Weekends and Bank Holidays
FTE	Full Time Equivalent
CSOC	Cyber Security Operations Centre

SIEM	Security Information and Event Management
True Positive	A true positive is any alert/incident that the CSOC deem necessary to raise out to the organisation/Service.
False Positive	A false positive is classified as: 1. An alert that was incorrectly flagged benign activity as a potential threat. 2. An alert that does not meet the CSOC's risk threshold to raise to the organisation or service owner. For the avoidance of doubt if the CSOC does not raise out the alert to the effected organisation or service this is classified as a false positive, even if the alert correctly triggered on the activity. This relates to the classification mechanisms of the current SIEM solution and could change.

5. Scope of requirement

5.1. The successful Supplier shall provide resource for 24x7 hours of coverage, to provide monitoring and security event alerting support. This will include periods of surge support.

5.2. The Supplier may be asked to increase capacity on the contract at any time. Upon request, the Supplier shall be capable of increasing the capacity of the Service incrementally as follows:

- An increase of 0.25 FTE within 28 days from the date of the written request by the Buyer.
- An increase of 0.5 FTE within 56 days from the date of the written request by the Buyer.
- Any increase greater than 0.5 FTE shall be worked out jointly between the Buyer and Supplier.

This will scale at a pro-rata rate agreed by both parties.

For the avoidance of doubt, this requirement could apply to either Office Hours or Out of Hours FTE uplift.

5.3. The successful Supplier will deliver the contract for an initial contract term of 36 months.

5.4. The Buyer reserves the right to extend the contract by up to 2 periods of 12 months each.

5.5. The high-level MoSCoW requirements detailed in Appendix B3 outline the requirements that must or should be met by a Supplier in order to be awarded the service.

5.6. Requirements marked as ‘must’ are mandatory requirements and a Supplier will not be awarded the service if they do not meet any of the requirements.

5.7. Any requirements marked as a ‘must’, must be met and maintained for the duration of contract. Lapse in compliance with any of the ‘must’ have requirements may be met with contract termination.

5.8. The Supplier must be adaptable to reasonable changes to the requirements over the course of the contract if these are required to effectively protect the National Health Service from Cyber-attacks.

6. The requirement

6.1. The Buyer will allocate an alert queue each morning to the Supplier for analysts to work through during the Office Hours period.

6.2. Out of Hours the Supplier will work across an out of hours alert queue allocated by the Buyer covering Critical and High, Medium and Low alerts - but prioritising Critical and High alerts.

6.3. The Supplier shall provide ‘one’ Full Time Equivalent (FTE) to cover the period of Office Hours (9-5). This cover will work as part of an extension of the existing Buyer's team. For the avoidance of doubt, the Buyer's expectation would be that this would be 1 FTE covering every regular office hour shift, made up of different shift analysts.

6.4. The Supplier shall provide 1.25 FTE to cover Out of Hours

covering Critical, High, Medium and Low alerts - but prioritising Critical and High alerts.

6.5. The Supplier shall maintain any required local documentation, local working instructions and playbooks over and above what is provided by the Buyer to their internal analysts.

6.6. The Supplier shall provide the Buyer with an estimated 150 hours' worth of surge call-off per 12-month period, to provide 1 FTE of additional resource to augment the BAU service. A minimum of 24 hours' notice will be given by the Buyer to the Supplier before this resource is required.

6.7. The Supplier will monitor CSOC SIEM and security tooling to provide security monitoring coverage to healthcare organisations as directed by the Buyer.

6.8. The security coverage is not exclusive to just the NHS England organisation and will include a broad selection of public sector healthcare across the United Kingdom, including Scotland, Wales and Northern Ireland.

6.9. In the event of a major cyber security incident the Buyer will provide the Supplier with alerting criteria that requires a heightened level of awareness from the Supplier. All Alerts that match this criterion will be considered Critical and the SLAs below will apply: -

6.9.1. Critical (Out of Hours) - Assigned within 15 minutes, closed or called out within 30 minutes;

6.9.2. High (Out of Hours) - Assigned within 15 minutes, closed or called out within 30 minutes.

6.10. In the event of a major cyber security incident deemed by the Buyer to require 'Heightened Awareness', there is a possibility that the Buyer requests that the Supplier contact the Buyer's on call resource directly opposed to the agreed Out of Hours escalation route.

6.11. In the event of a callout, the Buyer may request assistance from the Supplier in dealing with the activity that was called out. This includes but is not limited to device isolation. In these circumstances, the Supplier will be exempt from the SLAs as outlined in requirements CSOC/24x7/41, CSOC/24x7/42 and

CSOC/24x7/43 of Appendix B3 for the duration of that shift.

6.12. The Supplier must use the Buyer's incident management tool to record key data from any alerts, that are raised as incidents, as directed by the Buyer.

6.13. The Supplier shall utilise the Buyer's toolset. Including, but not limited to, Confluence, Jira, Splunk, Microsoft Sentinel, Microsoft Teams, Microsoft Defender and ServiceNow.

6.14. ‘Where the Authority wishes to commission additional work, specifically provision of cyber security services to support the CSOC programme, beyond the Statement of Requirements described in Order Schedule 20 (Specification), the Variation Form (including Appendix 1) in Joint Schedule 2 will be used by the Authority to communicate the specific requirements to the Supplier.

6.15. The Authority and Supplier will organise an initial scoping call covering the Variation details, timelines, business function(s) and high-level requirements. The Supplier shall respond with its proposal in the relevant sections of Appendix 1. Where the Authority agrees with the Supplier’s proposal, the Authority shall sign and return the Variation to the Supplier for counter signature via Atamis.

7. Key milestones and deliverables

7.1. The Supplier shall provide transition plans and support to both the Buyer and the Incumbent Supplier to onboard the Service.

7.2. The Supplier shall provide transition plans and support to both the Buyer and Incumbent Supplier to offboard the Service.

7.3. Including, but not limited to, analyst upskilling and documentation handover for a period of 8 weeks.

7.4. The Supplier shall be operationally ready to undertake handover activities with the Buyer and Incumbent Supplier within 4 weeks of contracts being signed.

Milestone/Deliverable	Description	Timeframe or Delivery Date
Kick off/Initiation Meeting	Contract commences with an opportunity to reconfirm scope and deliverables. To gain additional information and context regarding the Buyers organisation and to further clarify the scope	Within week 1 of Contract Award
Onboarding of Supplier Staff into Authority Tooling	Onboarding of Supplier Staff into Authority Tooling	Within week 4 of Contract Award
Ongoing SOC Operations	Daily operations of the SOC such as triaging and investigating alerts report.	Ongoing following the 8-week mobilisation and implementation (into BAU)
Monthly Reporting	Supplier will provide a monthly report of all incidents called out to the buyers on call team. Take part in the buyers KPI review of the suppliers SLA compliance.	Monthly reports
Quarterly Contract Management Meeting	With the use of an action tracker, review open actions and review any issues with the service. Assess the service received and review compliance with SLAs.	Quarterly virtual meeting

8. Monthly Management information/reporting

8.1. The Supplier should provide a monthly report of all incidents that were called out to the Buyer's on call team.

8.2. The Supplier should take part in monthly KPI reporting on compliance to SLAs and attend a monthly KPI review meeting.

9. Volumes

9.1. The Buyer expects a minimum Medium and Low Alert Closure Rate of 200 alerts over a 24-hour time period where such alerts are made available to the Supplier analysts.

9.2. The Buyer expects a minimum Critical and High Severity Alert Closure Rate of 50 alerts per Out of Hours period when such alerts are made available to the Supplier analysts.

9.3. If the actual volume of alerts exceeds the minimum volume of alerts, as outlined in either 9.1 or 9.2, by 50% or more for three consecutive 24-hour time periods, the Supplier reserves the right to increase resource capacity of the Service in line with Clause 5.2 to meet the required Service Levels.

10. Continuous improvement

10.1. The Supplier must be adaptable to reasonable changes to the requirements where these are deemed necessary to effectively protect the National Health Service from Cyber Attacks.

11. Quality

11.1. On a monthly basis the Buyer will review a random selection of 20% of Security Incidents classified by the Supplier analysts as true positive and raised into the Buyer's Incident Management platform. A 90% accuracy level must be met and maintained by the Supplier.

11.2. The Buyer will review a random selection of up to 5% of incidents classified by the Supplier Analyst as not true positive (as defined in 'True Positive definition'). A 99% accuracy level must be met and maintained by the Supplier.

11.3. The Supplier must not fail to raise to the Buyer any Critical alerts that due to the failure to raise and contain then result in a major incident and CIR deployment.

11.4. 95% of all alerts that are subject to SLA's should meet the SLA requirements as outlined in 6.9.

11.5. Performance will be monitored against all of the service levels detailed in section 14 of this Statement of Requirements, continued lapse of the requirements (except where the buyer and supplier agree that the lapse was reasonable and unavoidable) will result in the following: -

11.5.1. After one month of not meeting the SLA requirement the suppliers service lead must attend a meeting to discuss the non-compliance and agree mitigations including supplier analysts engaging in 4, 1 hour virtual training sessions

11.5.2. If the Supplier then fails to meet the SLA requirement for a second month, the service lead and a manager for the service must attend an in person meeting at the Buyers office in Leeds to discuss the non-compliance and agree further mitigations including; hosting a group of the buyers analysts at their site for a 2, full day training session in addition to 4 1 hour training sessions hosted virtually.

11.5.3. If the Supplier then fails to meet the SLA requirement for a third consecutive month the same intervention will then be repeated.

11.5.4. After 4 consecutive months of non-compliance to the required SLA, the Buyer reserve the right to terminate the contract.

12. Price

12.1. Prices are submitted excluding VAT via the e-Sourcing Suite Atamis as an uploaded Price Schedule Template (in the Commercial Envelope).

12.2. Expenses are not chargeable for any service received under this Contract.

13. Staff and Buyer service

13.1. All materials, content and artefacts created for the Buyer by the Supplier shall meet NHS England minimum standards and

conform to the Web Content Accessibility Guidelines (WCAG 2).

13.2. Supplier analysts must meet the following criteria:

- Computer Science / Cyber Security Degree or Cyber Security Apprenticeship (or equivalent qualifications/certifications) ; or
- 1 year of cyber security experience working as a SOC analyst; and
- Good written and verbal communication skills
- Problem Solver
- Analytical Thinker

Analysts not meeting these criteria may be added to the contract for training and upskilling purposes (in addition to daily allocated analysts on the Contract). For the avoidance of doubt, the CSOC are happy to develop less experienced resources, but these will not constitute part of the FTE requirements defined in this Contract until such times as the full criteria of 13.2 is met.

13.3. The Supplier shall declare all staff who will form the team delivering the Service to the Buyer prior to the commencement of the Service.

13.4. The Supplier and Buyer shall agree a process for the addition or removal of staff from the team delivering the Service, and all staff additions shall be subject to approval by the Buyer, which will not be unreasonably withheld. New resource joining the Service should be provided to the Buyer with at least 3 weeks lead time. This is to ensure that accounts and access can be configured within the Authority's systems for access to email and security tooling.

13.5. The Buyer can request the removal of Supplier analysts from the Service.

13.6. The Supplier shall ensure all staff changes maintain compliance with the staff, clearance, and training levels specified in these requirements.

13.7. The Supplier shall ensure continuity of delivery with the resources they allocate. For the avoidance of doubt the Buyer does not expect persistence in resourcing, however we would require that all staff are made known to the Buyer. The Buyer is happy for the Supplier to use a pool of resources with a level of persistence that

ensures continuity in delivery.

13.8. All persons who are in the pool of resources that could be allocated to deliver the Service shall have demonstrable experience of using Microsoft Sentinel and Microsoft Defender XDR as evidenced via Microsoft Sentinel (SC-200) certification.

13.9. All persons who are in the pool of resources that could be allocated to deliver the Service shall have demonstrable experience of using ServiceNow or an equivalent tool.

13.10. The Supplier shall provide a named technical liaison between the Buyer's CSOC leadership team and the Supplier's analyst resource pool who attends 2 hours a week of Buyer meetings to maintain effective ways of working and consistent communication between the two teams.

13.11. The Supplier shall host in person analyst shadowing sessions and workshops with the Buyer to allow analysts on both sides to maintain consistent ways of working. This shall be a minimum of 8, 6-hour sessions per 12 months. The Supplier to share how this would work.

13.12. The Supplier must have experience providing security monitoring services to government and healthcare environments.

14. Service levels and performance

14.1. The Supplier shall have and provide communications routes for a consistent named person(s) as a point of contact and Key Personnel to raise any Service escalations.

14.2. The following SLAs shall be applied. Critical and High Severity Alert Investigations Out of Hours:

14.2.1. Critical (Out of Hours) - Assigned within 15 minutes, closed or called out within 15 minutes from assignment.

14.2.2. High (Out of Hours) - Assigned within 15 minutes, closed or called out within 15 minutes from assignment.

14.3. KPIs and Service Levels for this contract are detailed below:

KPI/SLA	Service Area	KPI/SLA description	Target
1	Service Running	The following SLAs shall be applied to Critical and High SEVERITY ALERT investigations OUT OF HOURS: Critical (OUT OF HOURS) - Assigned within 15 minutes, closed or called out within 30 minutes High (OUT OF HOURS) - Assigned within 15 minutes, closed or called out within 30 minutes	95%
2	Service Running	The Buyer expects a minimum Critical and High SEVERITY ALERT Closure Rate of 50 alerts per OUT OF HOURS period when such alerts are made available to the Supplier analysts	95%
3	Service Running	The Buyer expects a minimum Medium and Low Alert Closure Rate of 200 alerts over a 24-hour time period where such alerts are made available to the Supplier analysts.	95%

14.4. The Buyer and Supplier will meet on a monthly basis and review the SLA's as outlined in the above table.

14.4.1. The Buyer will provide an SLA dashboard that will be available to the Supplier to review the SLA's.

14.4.2. Any breach of the SLA's will be thoroughly reviewed by the Buyer and Supplier and where both parties agree that the breach was unavoidable, there will be no consequences in terms of performance management or defaults against the Contract.

15. Security and confidentiality requirements

15.1. The Supplier shall hold and maintain List X accreditation for the full duration of the contractual term (allowing the Supplier to hold Secret Assets on behalf of government).

15.2. The Supplier shall ensure that all persons who are in the pool of resources that could be allocated to meet the operational requirements of this contract do so from within a List X accredited environment.

15.3. All documentation and Local Work Instructions created as part of the contract shall have the Intellectual Property rights reside with NHS England.

15.4. Data related to the Service in the form of service documentation and playbooks shall be retained for the time periods specified within the Data Retention Policy.

15.5. The Supplier shall be GDPR compliant.

15.6. The Supplier shall be Cyber Essentials Plus certified.

15.7. All persons who are in the pool of resources that could be allocated to the Service shall have full SC Clearance.

15.8. The Supplier shall ensure all persons who are in the pool of resources that could be allocated to deliver the Service have the capability to use a VPN and Reverse Proxy Portal with a UK exit point to access the toolset(s) provided by the Buyer.

15.9. The Supplier Service shall be configured to present a static publicly-routable External UK IP address for connectivity to the Buyer within 2 weeks of contracts being signed.

15.10. The Supplier shall provide their External IP Address for Allow Listing (for access via VPN / Remote Access Solution), within 2 weeks of the contracts being signed.

15.11. The Supplier analysts shall be able to use Microsoft Authenticator for two factor Authentication and Physical FIDO2 MFA tokens to access the Buyer's systems. FIDO2 tokens will be provided to the Supplier by the Buyer.

16. Payment and invoicing

16.1. Payment is 30 days from the invoice date.

16.2. The invoice will cover the services of the previous month.

16.3. Invoices should be submitted via electronic invoicing Tradeshift.

To register for Tradeshift please visit:- https://nhssbs.support.tradeshift.com and view the section called 'Getting Started with Tradeshift'; or in the limited circumstances where electronic invoicing is not possible, please email invoices and credit notes to the following email address sbs.apinvoicing@nhs.net with the billing address on the invoice being:

NHS ENGLAND
X24 PAYABLES K005
K005PO BOX 312
LEEDS
LS11 1HP

16.4. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs completed. Invoices should contain the following information.

- the purchase order number;
- a fixed BAU cost for the period, as per the submitted pricing schedule; and

- a breakdown of the surge costs for the period, detailed in accordance with the hourly rates and staff roles, as per the submitted pricing schedule.

Managing Public Money – Principles

16.5. NHS England have the responsibility to exercise proper stewardship of public funds, including compliance with the principles laid out in Managing Public Money. The standards ensure we are responsible for establishing and maintaining internal audit arrangements in accordance with the Public Sector Internal Audit Standards and have effective quality internal governance and sound financial management that demonstrates value for money.

16.6. Pricing will be determined based on the fixed BAU, cost plus the Surge Costs for that invoice period, as detailed in the pricing schedule submitted during the Call-Off Procedure.

16.7. Payments cannot be verified without the supporting evidence and therefore the invoice must correlate to the pricing schedule in the Contract.

17. Contract management

17.1. The Supplier shall commit to 4 Service reviews per 12 months, on a quarterly basis, these should be in person events at either Supplier or Buyer sites and may involve analysts for familiarisation.

18. Social Value

18.1. Social Value considerations form part of the Technical Response and can be found in the Social Value Envelope. Commitments made in the successful Supplier's response to the Social Value question in the Call-Off Procedure, will be included in the Order Contract.

19. Location

19.1. The Supplier **must** have a secure UK based office. All analysts

accessing the Buyers infrastructure must do so from this secure location.

CSOC 24/7 Protective Monitoring

Appendix B1 – High-Level Capability Requirements

Technical Must Haves	Pass/Fail
The Supplier must hold and maintain List X accreditation for the full duration of the contractual term.	
The Supplier must ensure that all persons who are in the pool of resources that could be allocated to meet the operational requirements of this contract do so from within a List X accredited environment.	
The Supplier must be GDPR compliant.	
The Supplier must be Cyber Essentials Plus certified.	
All persons who are in the pool of resources that could be allocated to the Service must have full SC Clearance.	
All materials, content and artefacts created for the Customer by the Supplier must meet NHS England minimum standards and conform to the Web Content Accessibility Guidelines (WCAG 2).	

The above Pass/Fail Technical 'Must Have' requirements are replicated in the Qualification Envelope in Atamis and referenced in Appendix B3 – CSOC 24x7 High-Level MoSCoW Requirements.

Please respond to the related questions within the Qualification Envelope. Each requirement above has its own question in the Qualification Envelope.

CSOC 24/7 Protective Monitoring

Appendix B3 – CSOC High-Level MoSCoW Requirements

Category	Ref	Requirement	Must / Should
Business/General/Business Policies	CSOC/24x7/01	The SUPPLIER shall provide transition plans and support to both the BUYER and the Incumbent SUPPLIER to onboard the SERVICE.	Must
Business/General/Business Policies	CSOC/24x7/02	The SUPPLIER shall provide transition plans and support to both the BUYER and Incumbent SUPPLIER to offboard the SERVICE. Including, but not limited to, analyst upskilling and documentation handover for a period of 8 weeks	Must
Business/General/Business Policies	CSOC/24x7/03	The SUPPLIER shall commit to 4 SERVICE reviews per 12 months, on a quarterly basis, these should be in person events at either SUPPLIER or BUYER sites, and may involve analysts for familiarisation.	Must
Business/General/Commercial	CSOC/24x7/04	All SUPPLIER invoices shall have a clear level of detail to support invoice approval and payments.	Must
Business/General/Constraints	CSOC/24x7/05	The SUPPLIER shall be operationally ready to undertake handover activities with the BUYER and Incumbent SUPPLIER within 4 weeks of contracts being signed.	Must
Business/General/Legal	CSOC/24x7/06	The SUPPLIER shall hold and maintain List X accreditation for the full duration of the contractual term, [allowing the SUPPLIER to hold Secret Assets on behalf of government].	Must
Business/General/Legal	CSOC/24x7/07	All materials, content and artefacts created for the BUYER by the SUPPLIER shall meet NHS England minimum standards and conform to the Web Content Accessibility Guidelines (WCAG 2)	Should
Business/General/Legal	CSOC/24x7/08	All documentation and Local Work Instructions created as part of the contract shall have the Intellectual Property rights reside with NHS England.	Must
Business/General/Legal	CSOC/24x7/09	Data related to the SERVICE in the form of service documentation and playbooks shall be retained for the time periods specified within the Data Retention Policy.	Must
Business/General/Legal	CSOC/24x7/10	The SUPPLIER shall be GDPR compliant.	Must
Business/General/Legal	CSOC/24x7/11	The SUPPLIER shall be Cyber Essentials Plus certified	Must
Staff/Training/Vetting	CSOC/24x7/12	All persons who are in the pool of resources that could be allocated to the SERVICE shall have full SC Clearance.	Must
Staff/Training/Vetting	CSOC/24x7/13	The SUPPLIER shall ensure that all persons who are in the pool of resources that could be allocated to meet the operational requirements of this contract do so from within a List X accredited environment.	Must
Staff/Training/Vetting	CSOC/24x7/14	SUPPLIER analysts must meet the following criteria: - Computer Science / Cyber Security Degree OR Cyber Security Apprenticeship - 1 year of cyber security experience working as a SOC analyst - Good written and verbal communication skills - Problem Solver - Analytical Thinker Analysts not meeting this criteria may be added for training and upskilling in addition to daily allocated analysts as per requirements CSOC/24x7/29 and CSOC/24x7/30 that meet this skill criteria. For the avoidance of doubt, the CSOC are happy to develop less experienced resources but these will not constitute part of the FTE requirements defined in CSOC/24x7/29 and CSOC/24x7/30.	Must
Staff/Training/Vetting	CSOC/24x7/15	The SUPPLIER shall provide and continually maintain and update the BUYER with the details of all persons who are in the pool of resources that could be allocated to deliver the SERVICE. This is so that the BUYER can validate minimum SC clearance before the resource is permitted to work on the SERVICE.	Must
Staff/Training/Vetting	CSOC/24x7/16	The SUPPLIER shall declare all staff who will form the team delivering the SERVICE to the BUYER prior to the commencement of the SERVICE.	Must
Staff/Training/Vetting	CSOC/24x7/17	The SUPPLIER and BUYER shall agree a process for the addition or removal of staff from the team delivering the SERVICE, and all staff additions shall be subject to approval by the BUYER, which will not be unreasonably withheld. New resource joining the SERVICE should be provided to the BUYER with at least 3 weeks lead time. This is to ensure that accounts and access can be configured within the Authority's systems for access to email and security tooling.	Must
Staff/Training/Vetting	CSOC/24x7/18	The BUYER can request the removal of SUPPLIER analysts from the SERVICE.	Must
Staff/Training/Vetting	CSOC/24x7/19	The SUPPLIER shall ensure all staff changes maintain compliance with the staff, clearance, and training levels specified in these requirements.	Must
Staff/Training/Vetting	CSOC/24x7/20	The SUPPLIER shall ensure continuity of delivery with the resources they allocate. For the avoidance of doubt the BUYER does not expect persistence in resourcing, however we would require that all staff are made known to the BUYER. The BUYER is happy for the SUPPLIER to use a pool of resources with a level of persistence that ensures continuity in delivery.	Must
Staff/Training/Vetting	CSOC/24x7/21	All persons who are in the pool of resources that could be allocated to deliver the SERVICE shall have demonstrable experience of using Microsoft Sentinel and Microsoft Defender XDR as evidenced via Microsoft Sentinel [SC-200] certification [this shall be demonstrated as part of the bid process].	Must
Staff/Training/Vetting	CSOC/24x7/22	The SUPPLIER shall ensure all persons who are in the pool of resources that could be allocated to deliver the SERVICE have the capability to use a VPN and Reverse Proxy Portal with a UK exit point to access the toolset(s) provided by the BUYER.	Must
Staff/Training/Vetting	CSOC/24x7/23	All persons who are in the pool of resources that could be allocated to deliver the SERVICE shall have demonstrable experience of using ServiceNow or an equivalent tool [this shall be demonstrated as part of the bid process].	Should
Staff/Training/Vetting	CSOC/24x7/24	The SUPPLIER shall provide a named technical liaison between the BUYER's CSOC leadership team and the SUPPLIER's analyst resource pool who attends 2 hours a week of BUYER meetings to maintain effective ways of working and consistent communication between the two teams.	Must
Staff/Training/Vetting	CSOC/24x7/25	The SUPPLIER shall host in person analyst shadowing sessions and workshops with the BUYER to allow analysts on both sides to maintain consistent ways of working. This shall be a minimum of 8, 6 hour sessions per 12 months. The SUPPLIER to share how this would work.	Must
Staff/Training/Vetting	CSOC/24x7/26	The SUPPLIER shall have and provide communications routes for a consistent named person(s) as a point of contact and KEY PERSONNEL to raise any SERVICE escalations.	Must
Staff/Training/Vetting	CSOC/24x7/27	The SUPPLIER must have experience providing security monitoring services to government and healthcare environments.	Must
Staff/Training/Vetting	CSOC/24x7/28	The SUPPLIER must have experience providing security monitoring services to critical national infrastructure	Must
Service Running	CSOC/24x7/29	The SUPPLIER shall provide 1 [one] Full Time Equivalent [FTE] to cover the period of OFFICE HOURS (9-5). This cover will work as part of an extension of the existing BUYER's team. For the avoidance of doubt, the BUYER's expectation would be that this would be 1 FTE covering every regular office hour shift, made up of different shift analysts.	Must
Service Running	CSOC/24x7/30	The SUPPLIER shall provide 1.25 FTE to cover OUT OF HOURS covering Critical and High, Medium and Low alerts - but prioritising Critical and High alerts.	Must
Service Running	CSOC/24x7/31	The SUPPLIER shall maintain any required local documentation, local working instructions and playbooks over and above what is provided by the BUYER to their internal analysts.	Should
Service Running	CSOC/24x7/32	The SUPPLIER shall provide the BUYER with 20 surge call-off days per 12 month period to provide 1 FTE of additional resouce to augment that given in CSOC/24x7/29 and CSOC/24x7/30. A minimum of 24 hours notice will be given by the BUYER to the SUPPLIER before this resource is required.	Must
Service Running	CSOC/24x7/33	The BUYER will allocate an alert queue each morning to the SUPPLIER for analysts to work through during the OFFICE HOURS period (CSOC/24x7/29)	Must
Service Running	CSOC/24x7/34	OUT OF HOURS the SUPPLIER will work across an out of hours alert queue allocated by the BUYER, but prioritised as per CSOC/24x7/30	Must
Service Running	CSOC/24x7/35	Upon request, the SUPPLIER shall be capable of increasing the capacity of the SERVICE incrementally as follows: - an increase of 0.25 FTE within 28 [twenty-eight] days from the date of the written request by the BUYER. - an increase of 0.5 FTE within 56 [fifty-six] days from the date of the written request by the BUYER. - Any increase greater than 0.5 FTE shall be worked out jointly between the BUYER and SUPPLIER. This will scale at a pro-rata rate agreed by both parties. For the avoidance of doubt, this requirement could apply to either OFFICE HOURS or OUT OF HOURS FTE uplift.	Must
Service Running	CSOC/24x7/36	The SUPPLIER will monitor CSOC SIEM and security tooling to provide security monitoring coverage to healthcare organisations as directed by the BUYER. The security coverage is not exclusive just the NHS England organisation, and will include a broad selection of public sector healthcare across the United Kingdom, including Scotland, Wales or Northern Ireland.	Must
Service Running	CSOC/24x7/37	In the event of a major cyber security incident the BUYER will provide the SUPPLIER with criteria that requires a heightened level of awareness from the SUPPLIER. All Alerts that match this criteria will be considered Critical and the SLAs outlined in CSOC/24x7/43 will apply.	Must
Seervice Running	CSOC/24x7/38	In the event of a major cyber security incident deemed by the BUYER to require 'Heightened Awareness' there is a possibility that the BUYER requests that the SUPPLIER contact the BUYER's on call resource directly opposed to the agreed OOH escalation route. As part of requirement CSOC/24x7/37	Must
Service Running	CSOC/24x7/39	In the event of a callout the BUYER may request assistance from the SUPPLIER in dealing with the activity that was called out. This includes but is not limited to device isolation. In these circumstances the SUPPLIER will be exempt from the SLAs as outlined in CSOC/24x7/41, CSOC/24x7/42 and CSOC/24x7/43 for the duration of that shift.	Must
Service Running	CSOC/24x7/40	The BUYER shall provide the SUPPLIER with SIEM outage contingency processes, in the event of a SIEM outage the SUPPLIER shall follow the contingency process.	Must
Service Standard Milestones	CSOC/24x7/41	The BUYER expects a minimum Medium and Low Alert Closure Rate of 200 alerts over a 24 [twenty-four] hour time period where such alerts are made available to the SUPPLIER analysts. As part of requirement CSOC/24x7/29.	Must
Service Standard Milestones	CSOC/24x7/42	The BUYER expects a minimum Critical and High SEVERITY ALERT Closure Rate of 50 alerts per OUT OF HOURS period when such alerts are made available to the SUPPLIER analysts. As part of requirement CSOC/24x7/30.	Must
Service Standard Milestones	CSOC/24x7/43	The following SLAs shall be applied to Critical and High SEVERITY ALERT investigations OUT OF HOURS: Critical (OUT OF HOURS) - Assigned within 15 minutes, closed or called out within 30 minutes High (OUT OF HOURS) - Assigned within 15 minutes, closed or called out within 30 minutes	Must
Service Tooling	CSOC/24x7/44	The SUPPLIER must use the BUYER's incident management tool to record key data from any alerts, that are raised as incidents, as directed by the BUYER.	Must
Service Tooling	CSOC/24x7/45	The SUPPLIER shall utilise the BUYER's toolset. Including, but not limited to, Confluence, Jira, Splunk, Microsoft Sentinel, Microsoft Teams, Microsoft Defender and ServiceNow.	Must
Service Tooling	CSOC/24x7/46	The SUPPLIER SERVICE shall be configured to present a static publicly-routable External UK IP address for connectivity to the BUYER within 2 weeks of contracts being signed.	Must
Service Tooling	CSOC/24x7/47	The SUPPLIER shall provide their External IP Address for Allow Listing, [for access via VPN / Remote Access Solution] within 2 weeks of the contracts being signed.	Must
Service Tooling	CSOC/24x7/48	The SUPPLIER analysts shall be able to use Microsoft Authenticator for two factor Authentication and Physical FIDO2 MFA tokens to access the BUYER's systems. FIDO2 tokens will be provided to the SUPPLIER by the BUYER.	Must
Service Running	CSOC/24x7/49	Supplier must be adaptable to reasonable changes to processes and alerting as required to best protect the system.	Must
Service Running	CSOC/24x7/50	The BUYER will review a random selection of 20% of Security Incidents classified by the SUPPLIER analysts as true positive and raised into the BUYERS Incident Management platform. A 90% accuracy level must be met and maintened by the SUPPLIER.	Must
Service Running	CSOC/24x7/51	The BUYER will review a random selection of up to 5% of incidents classified by the SUPPLIER Analyst as NOT true positive (as defined in [TRUE POSITIVE definition]. A 99% accuracy level must be met and maintaines SUPPLIER.	Must
Service Running	CSOC/24x7/52	The SUPPLIER must not fail to raise to the BUYER any Critical alerts that due to the failure to raise and contain then result in a major incident and CIR deployment.	Must
Service Running	CSOC/24x7/53	95% of all alerts that are subject to SLA's should meet the SLA requirements as outlined in 43.	Must
Service Running	CSOC/24x7/54	All 'must requirements must be met and maintained for the duration of the contract	Must
Reporting	CSOC/24x7/55	The SUPPLIER should provide a monthly report of all incidents that were called out to the BUYERS on call team.	Should
Staff/Training/Vetting	CSOC/24x7/56	The SUPPLIER must have a secure UK based office. All analysts accessing the BUYERS infrastructure must do so from this secure location.	Must

Appendix B4-SOC Analyst Role Profile

SOC ANALYST

Role summary and profile

About this role

The SOC Analyst provides an initial analysis on security data to identify potential threats and formulate recommendations and actions to consider in order to remediate and respond. They support senior colleagues in assessing, planning, and advising stakeholders on security measures that will help protect NHS England from security breaches and attacks on its computer networks and systems. The role will be working alongside the Analyst pool as part of the Protective Monitoring team within the Detect & Respond pillar. This will involve the triaging and investigation of different alerts using SIEM tools and raising security incidents as required.

Professional Competencies

Knowledge, Skills and Qualifications

Essential

Information Technology (IT) Security Policies (1)
Knowledge of IT security policies, standards, and procedures; ability to utilise a variety of administrative skill sets and technical knowledge to ensure cyber security compliance.

Information Security Management (2)
Knowledge of the processes, tools and techniques of information security management, ability to deploy and monitor information security systems, as well as detect, resolve and prevent violations of IT security, to protect organisational data.

Information Security Technologies (1)
Knowledge of technologies and technology-based solutions dealing with information security issues; ability to apply these in protecting information security across the organisation.

Information Assurance (1)
Knowledge of and the ability to protect information and information systems while ensuring their confidentiality, integrity and availability.

Digital Threat Management (2)
Knowledge of techniques, approaches and processes of digital threats; ability to detect, monitor, analyse and prevent digital threats.

Security Information and Event Management (SIEM) (1)
Knowledge of concept, procedures and processes of Security Information and Event Management (SIEM); ability to utilise related applications to protect organisational networks from cyber risks.

Intrusion Detection and Prevention (2)
Knowledge of tools, techniques and processes of intrusion detection and prevention; ability to detect, resolve and prevent intrusion behaviours to protect organisational networks.

Information Security Operation Centre (ISOC) (1)
Knowledge of modules, processes and technologies of Information Security Operation Centre (ISOC); ability to detect, response and utilise related platform and applications to perform cyber security initiatives.

Endpoint Security (1)
Proven knowledge of concept, issues and techniques of endpoint security; ability to ensure security compliance of endpoint devices in various circumstances.

Email Security
Proven knowledge of concept, issues and techniques of email security; ability to detect, monitor, analyse and prevent unauthorised access, loss or compromise of business email accounts.

Cloud Security
Proven knowledge of concept, issues and techniques of Cloud security; ability to ensure security compliance of cloud infrastructure in various circumstances.

Desirable

Computer Forensics (1)
Knowledge of technologies, methods and tools of forensics investigations for IT security violations or potential threats; ability to identify, uncover and evaluate violations, warning reports, suspected incidents and insidious events.

Digital Forensic Tools (1)
Knowledge of and ability to utilise a variety of specific tools for collecting, analysing, and presenting digital-related evidence.

Qualifications

Essential

- Post-graduate level degree or equivalent level of experience (3 years' industry experience or apprenticeship in Cyber Security).
- Evidence of continuous professional development in Cyber Security.
- Microsoft Certified: Security Operations Analyst Associate (SC-200)

Desirable

- CompTIA Security+
- Comptia Network+
- CompTIA CySA+ (Cybersecurity Analyst)

Appendix B5-Senior SOC Analyst Role Profile

Senior SOC Analyst

Role summary and profile

About this role

The Senior SOC Analyst role provides second line security analytics and acts as an escalation point for the SOC analysts. They work within the Protective monitoring team within the Detect & Respond pillar. They work with the area leads to provide intermediary support between the client and supplier SOC analysts.

- Act as an escalation point for SOC Analysts for incidents and investigations.
- Offer mentorship and guidance to SOC Analysts to support others and their own growth and development.
- Keep up to date with the latest security and technology developments, including researching and evaluating emerging cyber security threats and ways to manage them.
- Apply experience and knowledge to assist with investigations of triggered security alerts.
- Assist with the refinement of Use Cases and identification of areas for improvement of overall security posture.

Professional Competencies

Knowledge, Skills and Qualifications

Essential

Information Technology (IT) Security Policies (2)
Proven knowledge of IT security policies, standards, and procedures; ability to utilise a variety of administrative skill sets and technical knowledge to ensure cyber security compliance.

Information Security Management (2)
Demonstrable knowledge of the processes, tools and techniques of information security management, ability to deploy and monitor information security systems, as well as detect, resolve and prevent violations of IT security, to protect organisational data.

Digital Forensic Tools (2)
Demonstrable knowledge of and ability to utilize a variety of specific tools for collecting, analysing, and presenting digital-related evidence.

Information Security Operation Centre (ISOC) (2)
Working knowledge of modules, processes and technologies of Information Security Operation Centre (ISOC); ability to detect, response and utilise related platform and applications to perform cyber security initiatives.

Information Security Technologies (2)
Demonstrable knowledge of technologies and technology-based solutions dealing with information security issues; ability to apply these in protecting information security across the organization.

Computer Forensics (1)
Introductory knowledge of technologies, methods and tools of forensics investigations for IT security violations or potential threats; ability to identify, uncover and evaluate violations, warning reports, suspected incidents and insidious events.

Information Assurance (1)
Basic knowledge of and the ability to protect information and information systems while ensuring their confidentiality, integrity and availability.

Application Security (2)
Working knowledge of the tools and processes for maintaining application security; ability to design and implement security programs to prevent data loss and access intrusion from web and mobile applications.

Digital Threat Management (2)
Proven knowledge of techniques, approaches and processes of digital threats; ability to detect, monitor, analyse and prevent digital threats.

Endpoint Security (1)
Proven knowledge of concept, issues and techniques of endpoint security; ability to ensure security compliance of endpoint devices in various circumstances.

Email Security

Proven knowledge of concept, issues and techniques of email security; ability to detect, monitor, analyse and prevent unauthorised access, loss or compromise of business email accounts.

Cloud Security
Proven knowledge of concept, issues and techniques of Cloud security; ability to ensure security compliance of cloud infrastructure in various circumstances.

Data Privacy (1)
Introductory knowledge of and ability to protect an organisation's data to ensure privacy during the process of storage and communication.

Security Information and Event Management (SIEM) (2)
Working knowledge of concept, procedures and processes of Security Information and Event Management (SIEM); ability to utilise related applications to protect organisational networks from cyber risks.

Intrusion Detection and Prevention (2)
Proven knowledge of tools, techniques and processes of intrusion detection and prevention; ability to detect, resolve and prevent intrusion behaviours to protect organisational networks.

IT Incident Management (2)
Demonstrable knowledge of and ability to investigate, troubleshoot, resolve and prevent the recurrence of incidents that interfere with the normal delivery of IT services.

Qualifications

Essential

- Post-graduate level degree or equivalent level of experience.
- Evidence of continuous professional development.
- Microsoft Certified: Security Operations Analyst Associate (SC-200)

In addition, we expect the Post Holder to specialise in one of the following areas:

- CompTIA Security+
- Comptia Network+

- CompTIA CySA+ (Cybersecurity Analyst)
- SANS SEC401

Order Schedule 22 – Secret Matters

Associated definitions:

In this Order Schedule 22, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Document"	includes specifications, plans, drawings, photographs and books;
"Secret Matter"	means any matter connected with or arising out of the performance of this Order Contract which has been, or may hereafter be, by a notice in writing given by the Customer to the Supplier be designated 'top secret', 'secret', or 'confidential';
"Servant"	where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called.

1. Disclosure

1.1 The Supplier shall not, either before or after the completion or termination of this Order Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a Secret Matter being:

1.1.1 without the prior consent in writing of the Buyer, disclosed to or acquired by a person who is an alien or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;

1.1.2 disclosed to or acquired by a person as respects whom the Buyer has given to the Supplier a notice in writing which has not been cancelled stating that the Buyer requires that Secret Matters shall not be disclosed to that person;

1.1.3 without the prior consent in writing of the Buyer, disclosed to or acquired by any person who is not a Servant of the Supplier; or

1.1.4 disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Order Contract that such person shall have the information.

2. Safeguarding

2.1 Without prejudice to the provisions of Paragraph 1, the Supplier shall, both before and after the completion or termination of this Order Contract, take all reasonable steps to ensure:

2.1.1 no such person as is mentioned in Paragraph 1.1, 1.1.1 or 1.1.2, thereof shall have access to any item or Document under the control

of the Supplier containing information about a Secret Matter except with the prior consent in writing of the Buyer;

2.1.2 that no visitor to any premises in which there is any item to be supplied under this Order Contract or where Goods are being supplied shall see or discuss with the Supplier or any person employed by him any Secret Matter unless the visitor is authorised in writing by the Buyer so to do;

2.1.3 that no photograph of any item to be supplied under this Order Contract or any portions of the Goods shall be taken except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, and that no such photograph shall, without such consent, be published or otherwise circulated;

2.1.4 that all information about any Secret Matter and every Document, model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, no copies of or extracts from any such Document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such Document, model or item shall be placed thereon; and

2.1.5 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Customer of any such Document, model or item as is mentioned in Paragraph 2.1.4, that Document, model or item (including all copies of or extracts therefrom) shall forthwith be delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

3. Decision of the Buyer

3.1 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Order Schedule 22 shall be final and conclusive.

4. Particulars of People

4.1 If and when directed by the Buyer, the Supplier shall furnish full particulars of all people who are at any time concerned with any Secret Matter.

5. Official Secrets Act

5.1 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of the Order Contract.

6. Information concerning the Contract

6.1 If, at any time either before or after the expiry or termination of this Order Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Order Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

7. Duty to observe obligations

7.1 The Supplier shall place every person employed by it, other than a Sub contractor, who in its opinion has or will have such knowledge of any Secret Matter as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that Secret Matter as are imposed on the Supplier by Paragraphs 1 and 2 and shall, if directed by the Buyer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any Secret Matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Order Schedule 22 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Supplier with all necessary particulars.

8. Sub-Contract Obligations

8.1 The Supplier shall, if directed by the Buyer, include in the Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Order Schedule 22, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:

8.1.1 give such notices, directions, requirements and decisions to its Sub Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Order Schedule 22 into operation in such cases and to such extent as the Buyer may direct;

8.1.2 if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Order Schedule 22, notify such breach forthwith to the Customer; and

8.1.3 if and when so required by the Buyer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Paragraph 11.

9. Information to the Buyer

9.1 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Order Schedule 22 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Order Contract or in which there is or will be any item to be supplied under this Order Contract, and also to inspect any Document or item in any such premises or which is being made or used for the purposes of this Order Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

10. Exclusion

10.1 Nothing in this Order Schedule 22 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

11. Grounds for Termination

11.1 If the Buyer shall consider that any of the following events has occurred:

11.1.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Order Schedule 22; or

11.1.2 that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Buyer, or with any department or person acting on behalf of the Crown; or

11.1.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Paragraph

11.1.4 information about a Secret Matter has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information;

11.1.5 and shall also decide that the interests of the state require the termination of this Order Contract, the Buyer may by notice in writing terminate this Order Contract forthwith.

12. Buyer Decision to Terminate

12.1 A decision of the Buyer to terminate this Order Contract in accordance with the provisions of Paragraph 11 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any

way to the event or considerations upon which the Buyer's decision is based.

13. Supplier's notice

13.1 The Supplier may within five (5) Working Days of the termination of this Order Contract in accordance with the provisions of Paragraph 11, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Paragraphs 11.1.1, 11.1.2 or 11.1.3 and to give particulars of that event; and

13.2 the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

14. Matters pursuant to termination

14.1 The termination of this Order Contract pursuant to Paragraph 11 shall be without prejudice to any rights of either Party which shall have accrued before the date of such termination;

14.2 The Supplier shall be entitled to be paid for any work or thing done under this Order Contract and accepted but not paid for by the Buyer at the date of such termination either at the price which would have been payable under this Order Contract if the Order Contract had not been terminated, or at a reasonable price;

14.3 The Buyer may take over any work or thing done or made under this Order Contract (whether completed or not) and not accepted at the date of such termination which the Buyer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Order Schedule 22 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Buyer, deliver any work or thing taken over under this Paragraph 14.3, and take all such other steps as may be reasonably necessary to enable the Buyer to have the full benefit of any work or thing taken over under this Paragraph 14.3 ; and

14.4 Save as aforesaid, the Supplier shall not be entitled to any payment from the Buyer after the termination of this Order Contract.

15. Rights & Obligations after Termination

15.1 If, after notice of termination of this Order Contract pursuant to the provisions of Paragraph 11:

15.1.1 the Buyer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Paragraph 13.1; or

15.1.2 the Buyer shall state in the statement and particulars detailed in Paragraph 13.2 that the event upon which the Buyer's

decision to terminate this Order Contract was based is an event mentioned in Paragraph.11.1.3,

15.1.3 the respective rights and obligations of the Supplier and the Buyer shall be terminated in accordance with the following provisions:

15.2 the Buyer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Order Contract under the provisions of Paragraph 11 and properly provided by or supplied to the Supplier for the performance of this Order Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Buyer, elect to retain;

15.3 the Supplier shall prepare and deliver to the Buyer within an agreed period or in default of agreement within such period as the Buyer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Buyer and shall deliver such materials and items in accordance with the directions of the Buyer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;

15.4 the Buyer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Order Contract to the extent to which the said commitments, liabilities or expenditure would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Order Contract;

15.5 if hardship to the Supplier should arise from the operation of this Paragraph 15 it shall be open to the Supplier to refer the circumstances to the Buyer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Buyer on any matter arising out of this Paragraph 15.5 shall be final and conclusive; and

15.6 subject to the operation of Paragraphs15.2, 15.3, 15.4, and 15.5 termination of this Order Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.

Crown Commercial Service

Core Terms - DPS

1. Definitions used in the contract

1.1 Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

2.1 The Supplier is eligible for the award of Order Contracts during the DPS Contract Period.

2.2 CCS doesn't guarantee the Supplier any exclusivity, quantity or value of work under the DPS Contract.

2.3 CCS has paid one penny to the Supplier legally to form the DPS Contract. The Supplier acknowledges this payment.

2.4 If the Buyer decides to buy Deliverables under the DPS Contract it must use DPS Schedule 7 (Order Procedure) and must state its requirements using DPS Schedule 6 (Order Form Template and Order Schedules). If allowed by the Regulations, the Buyer can:

- make changes to DPS Schedule 6 (Order Form Template and Order Schedules)
- create new Order Schedules
- exclude optional template Order Schedules
- use Special Terms in the Order Form to add or change terms

2.5 Each Order Contract:

- is a separate Contract from the DPS Contract
- is between a Supplier and a Buyer
- includes Core Terms, Schedules and any other changes or items in the completed Order Form
- survives the termination of the DPS Contract

2.6 Where the Supplier is approached by an eligible buyer requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this DPS Contract before accepting their order. The Supplier will promptly notify CCS if the eligible buyer won't use this DPS Contract.

2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

2.8 The Supplier won't be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:

- verify the accuracy of the Due Diligence Information
- properly perform its own adequate checks

2.9 CCS and the Buyer won't be liable for errors, omissions or misrepresentation of any information.

2.10 The Supplier warrants and represents that all statements made and documents submitted as part of

the procurement of Deliverables are and remain true and accurate.

2.11 An Order Contract can only be created using the electronic procedures described in the OJEU Notice as required by the Regulations.

2.12 A Supplier can only receive Orders under the DPS Contract while it meets the basic access requirements for the DPS stated in the OJEU Notice. CCS can audit whether a Supplier meets the basic access requirements at any point during the DPS Contract Period.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

- that comply with the Specification, the DPS Application and, in relation to an Order Contract, the Order Tender (if there is one)
- to a professional standard
- using reasonable skill and care
- using Good Industry Practice
- using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract
- on the dates agreed
- that comply with Law

3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.

3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.

3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.

3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.

3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.

3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.

3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.

3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.

3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.

3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.

3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with Clause 3. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.

3.3 Services clauses

3.3.1 Late Delivery of the Services will be a Default of an Order Contract.

3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.

3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.

3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.

3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.

3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4 Pricing and payments

4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.

4.2 CCS must invoice the Supplier for the Management Levy and the Supplier must pay it using the process in DPS Schedule 5 (Management Levy and Information).

4.3 All Charges and the Management Levy:

- exclude VAT, which is payable on provision of a valid VAT invoice
- include all costs connected with the Supply of Deliverables

4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.

4.5 A Supplier invoice is only valid if it:

- includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer
- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)
- does not include any Management Levy (the Supplier must not charge the Buyer in any way for the Management Levy)

4.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.

4.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, CCS or the Buyer can publish the details of the late payment or non-payment.

4.8 If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables and that cost is reimbursable by the Buyer, then CCS or the Buyer may either:

- require the Supplier to replace its existing commercial terms with the more favourable terms offered for the relevant items
- enter into a direct agreement with the Subcontractor or third party for the relevant item

4.9 If CCS or the Buyer uses Clause 4.8 then the Charges must be reduced by an agreed amount by using the Variation Procedure.

4.10 CCS and the Buyer's right to enter into a direct agreement for the supply of the relevant items is subject to both:

- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Charges excluding any unavoidable costs that must be paid by the Supplier for the substituted item, including any licence fees or early termination charges

4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they're ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- neither CCS or the Buyer can terminate a Contract under Clause 10.4.1
- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Authority Cause
- mitigated the impact of the Authority Cause

6. Record keeping and reporting

6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.

6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the End Date.

6.3 The Supplier must allow any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit.

6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- tell the Relevant Authority and give reasons
- propose corrective action
- provide a deadline for completing the corrective action

6.6 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:

- the methodology of the review
- the sampling techniques applied
- details of any issues

- any remedial action taken

6.7 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

7.1 The Supplier Staff involved in the performance of each Contract must:

- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises

7.2 Where a Buyer decides one of the Supplier's Staff isn't suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.

7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.

7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.

7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- it has full capacity and authority to enter into and to perform each Contract
- each Contract is executed by its authorised representative
- it is a legally valid and existing organisation incorporated in the place it was formed
- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract
- it does not have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract
- it is not impacted by an Insolvency Event
- it will comply with each Order Contract

8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.

8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:

- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract
- non-payment by the Supplier of any tax or National Insurance

8.4 All claims indemnified under this Contract must use Clause 26.

8.5 CCS or a Buyer can terminate the Contract for breach of any warranty or indemnity where they are entitled to do so.

8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.

8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier

9.2 Any New IPR created under an Order Contract is owned by the Buyer. The Buyer gives the Supplier i) a licence to use any Buyer Existing IPRs and New IPR during the Order Contract Period for the purpose of fulfilling its obligations under the Order Contract, and ii) a licence to use the New IPRs (excluding any Information which is the Buyers Confidential information or which is subject to the Data Protection Legislation) after the Order Contract period on the terms set out in the Open Government Licence.

9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.

9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.

9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:

- obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR

- replace or modify the relevant item with substitutes that don't infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the contract

10.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.

10.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.3 Ending the contract without a reason

10.3.1 CCS has the right to terminate the DPS Contract at any time without reason or liability by giving the Supplier at least 30 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.3.2 Each Buyer has the right to terminate their Order Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.4 When CCS or the buyer can end a contract

10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:

- there's a Supplier Insolvency Event
- there's a Contract Default that is not corrected in line with an accepted Rectification Plan
- the Relevant Authority rejects a Rectification Plan or the Supplier does not provide it within 10 days of the request
- there's any material default of the Contract
- there's a Default of Clauses 2.10, 9, 14, 15, 27, 32 or DPS Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract
- there's a consistent repeated failure to meet the Performance Indicators in DPS Schedule 4 (DPS Management)
- there's a Change of Control of the Supplier which isn't pre-approved by the Relevant Authority in writing
- there's a Variation to a Contract which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes)
- if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning of the European Union (TFEU) to declare that the Contract should not have been awarded to the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them

10.4.2 CCS may terminate the DPS Contract if a Buyer terminates an Order Contract for any of the reasons listed in Clause 10.4.1.

10.4.3 If there is a Default, the Relevant Authority can, without limiting its other rights, request that the Supplier provide a Rectification Plan.

10.4.4 When the Relevant Authority receives a requested Rectification Plan it can either:

- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties

10.4.5 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:

- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days

10.4.6 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Relevant Authority has the right to immediately terminate the Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the contract ends

Where the Relevant Authority terminates a Contract under Clause 10.4.1 all of the following apply:

10.5.1 The Supplier is responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.
10.5.2 The Buyer's payment obligations under the terminated Contract stop immediately.
10.5.3 Accumulated rights of the Parties are not affected.
10.5.4 The Supplier must promptly delete or return the Government Data except where required to retain copies by law.
10.5.5 The Supplier must promptly return any of CCS or the Buyer's property provided under the terminated Contract.
10.5.6 The Supplier must, at no cost to CCS or the Buyer, co-operate fully in the handover and re-procurement (including to a Replacement Supplier).
10.5.7 The following Clauses survive the termination of each Contract: 3.2.10, 6, 7.2, 9, 11, 14, 15, 16, 17, 18, 34, 35 and any Clauses and Schedules which are expressly or by implication intended to continue.

10.6 When the supplier can end the contract

10.6.1 The Supplier can issue a Reminder Notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate an Order Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the annual Contract Value within 30 days of the date of the Reminder Notice.

10.6.2 If a Supplier terminates an Order Contract under Clause 10.6.1:

- the Buyer must promptly pay all outstanding Charges incurred to the Supplier
- the Buyer must pay the Supplier reasonable committed and unavoidable Losses as long as the

Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated

- Clauses 10.5.4 to 10.5.7 apply

10.7 When subcontracts can be ended

At the Buyer's request, the Supplier must terminate any Subcontracts in any of the following events:

- there is a Change of Control of a Subcontractor which isn't pre-approved by the Relevant Authority in writing
- the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 10.4
- a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Relevant Authority

10.8 Partially ending and suspending the contract

10.8.1 Where CCS has the right to terminate the DPS Contract it can suspend the Supplier's ability to accept Orders (for any period) and the Supplier cannot enter into any new Order Contracts during this period. If this happens, the Supplier must still meet its obligations under any existing Order Contracts that have already been signed.

10.8.2 Where CCS has the right to terminate a DPS Contract it is entitled to terminate all or part of it.

10.8.3 Where the Buyer has the right to terminate an Order Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends a Contract it can provide the Deliverables itself or buy them from a third party.

10.8.4 The Relevant Authority can only partially terminate or suspend a Contract if the remaining parts of that Contract can still be used to effectively deliver the intended purpose.

10.8.5 The Parties must agree any necessary Variation required by Clause 10.8 using the Variation Procedure, but the Supplier may not either:

- reject the Variation
- increase the Charges, except where the right to partial termination is under Clause 10.3

10.8.6 The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under Clause 10.8.

11. How much you can be held responsible for

11.1 Each Party's total aggregate liability in each Contract Year under this DPS Contract (whether in tort, contract or otherwise) is no more than £100,000.

11.2 Each Party's total aggregate liability in each Contract Year under each Order Contract (whether in tort,

contract or otherwise) is no more than the greater of £1 million or 150% of the Estimated Yearly Charges unless specified in the Order Form.

11.3 No Party is liable to the other for:

- any indirect Losses
- Loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect)

11.4 In spite of Clause 11.1 and 11.2, neither Party limits or excludes any of the following:

- its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors
- its liability for bribery or fraud or fraudulent misrepresentation by it or its employees
- any liability that cannot be excluded or limited by Law
- its obligation to pay the required Management Levy

11.5 In spite of Clauses 11.1 and 11.2, the Supplier does not limit or exclude its liability for any indemnity given under Clauses 7.5, 8.3, 9.5, 31.3 or Order Schedule 2 (Staff Transfer) of a Contract.

11.6 Each Party must use all reasonable endeavours to mitigate any Loss or damage which it suffers under or in connection with each Contract, including any indemnities.

11.7 When calculating the Supplier's liability under Clause 11.1 or 11.2 the following items will not be taken into consideration:

- Deductions
- any items specified in Clause 11.5

11.8 If more than one Supplier is party to a Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

12. Obeying the law

12.1 The Supplier must use reasonable endeavours to comply with the provisions of Joint Schedule 5 (Corporate Social Responsibility).

12.2 To the extent that it arises as a result of a Default by the Supplier, the Supplier indemnifies the Relevant Authority against any fine or penalty incurred by the Relevant Authority pursuant to Law and any costs incurred by the Relevant Authority in defending any proceedings which result in such fine or penalty.

12.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, Clause 12.1 and Clauses 27 to 32.

13. Insurance

The Supplier must, at its own cost, obtain and maintain the Required Insurances in Joint Schedule 3 (Insurance Requirements) and any Additional Insurances in the Order Form.

14. Data protection

14.1 The Supplier must process Personal Data and ensure that Supplier Staff process Personal Data only in accordance with Joint Schedule 11 (Processing Data).

14.2 The Supplier must not remove any ownership or security notices in or relating to the Government Data.

14.3 The Supplier must make accessible back-ups of all Government Data, stored in an agreed off-site location and send the Buyer copies every 6 Months.

14.4 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.

14.5 If at any time the Supplier suspects or has reason to believe that the Government Data provided under a Contract is corrupted, lost or sufficiently degraded, then the Supplier must notify the Relevant Authority and immediately suggest remedial action.

14.6 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Relevant Authority may either or both:

- tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Relevant Authority receives notice, or the Supplier finds out about the issue, whichever is earlier
- restore the Government Data itself or using a third party

14.7 The Supplier must pay each Party's reasonable costs of complying with Clause 14.6 unless CCS or the Buyer is at fault.

14.8 The Supplier:

- must provide the Relevant Authority with all Government Data in an agreed open format within 10 Working Days of a written request
- must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading
- must securely destroy all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice

- securely erase all Government Data and any copies it holds when asked to do so by CCS or the Buyer unless required by Law to retain it
- Indemnifies CCS and each Buyer against any and all Losses incurred if the Supplier breaches Clause 14 and any Data Protection Legislation.

14.9. 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.

14.10 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.

14.11. Any cost arising out of the actions of the Parties taken in compliance with the provisions of Clause 14.10 shall be borne by the Parties as follows:

14.11.1 by the Supplier, where the Malicious Software originates from the software provided 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 Relevant Authority when provided to the Supplier; and

14.11.2. by the Relevant Authority, if the Malicious Software originates from the software provided by the Relevant Authority or the Government Data (whilst the Government Data was under the control of the Relevant Authority). 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.

15. What you must keep confidential

15.1 Each Party must:

- keep all Confidential Information it receives confidential and secure
- not disclose, use or exploit the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent, except for the purposes anticipated under the Contract
- immediately notify the Disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information

15.2 In spite of Clause 15.1, a Party may disclose Confidential Information which it receives from the Disclosing Party in any of the following instances:

- where disclosure is required by applicable Law or by a court with the relevant jurisdiction if the Recipient Party notifies the Disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure
- if the Recipient Party already had the information without obligation of confidentiality before it was disclosed by the Disclosing Party

- if the information was given to it by a third party without obligation of confidentiality
- if the information was in the public domain at the time of the disclosure
- if the information was independently developed without access to the Disclosing Party's Confidential Information
- to its auditors or for the purposes of regulatory requirements
- on a confidential basis, to its professional advisers on a need-to-know basis
- to the Serious Fraud Office where the Recipient Party has reasonable grounds to believe that the Disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier Staff must enter into a direct confidentiality agreement with the Relevant Authority at its request.

15.4 CCS or the Buyer may disclose Confidential Information in any of the following cases:

- on a confidential basis to the employees, agents, consultants and contractors of CCS or the Buyer
- on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that CCS or the Buyer transfers or proposes to transfer all or any part of its business to
- if CCS or the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions
- where requested by Parliament
- under Clauses 4.7 and 16

15.5 For the purposes of Clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in Clause 15.

15.6 Transparency Information is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contracts or any part of them in any way, without the prior written consent of the Relevant Authority and must take all reasonable steps to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Relevant Authority within 48 hours if it receives a Request For Information.

16.2 Within the required timescales the Supplier must give CCS and each Buyer full co-operation and information needed so the Buyer can:

- publish the Transparency Information
- comply with any Freedom of Information Act (FOIA) request
- comply with any Environmental Information Regulations (EIR) request

16.3 The Relevant Authority may talk to the Supplier to help it decide whether to publish information under Clause 16. However, the extent, content and format of the disclosure is the Relevant Authority's decision, which does not need to be reasonable.

17. Invalid parts of the contract

If any part of a Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from that Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it's valid or enforceable.

18. No other terms apply

The provisions incorporated into each Contract are the entire agreement between the Parties. The Contract replaces all previous statements and agreements whether written or oral. No other provisions apply.

19. Other people's rights in a contract

No third parties may use the Contracts (Rights of Third Parties) Act (CRTPA) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

20. Circumstances beyond your control

20.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under a Contract while the inability to perform continues, if it both:

- provides a Force Majeure Notice to the other Party
- uses all reasonable measures practical to reduce the impact of the Force Majeure Event

20.2 Either party can partially or fully terminate the affected Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.

20.3 Where a Party terminates under Clause 20.2:

- each party must cover its own Losses
- Clause 10.5.2 to 10.5.7 applies

21. Relationships created by the contract

No Contract creates a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

22. Giving up contract rights

A partial or full waiver or relaxation of the terms of a Contract is only valid if it is stated to be a waiver in writing to the other Party.

23. Transferring responsibilities

23.1 The Supplier can not assign a Contract without the Relevant Authority's written consent.

23.2 The Relevant Authority can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Relevant Authority.

23.3 When CCS or the Buyer uses its rights under Clause 23.2 the Supplier must enter into a novation agreement in the form that CCS or the Buyer specifies.

23.4 The Supplier can terminate a Contract novated under Clause 23.2 to a private sector body that is experiencing an Insolvency Event.

23.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.

23.6 If CCS or the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of Subcontractors at all levels of the supply chain including:

- their name
- the scope of their appointment
- the duration of their appointment

24. Changing the contract

24.1 Either Party can request a Variation to a Contract which is only effective if agreed in writing and signed by both Parties.

24.2 The Supplier must provide an Impact Assessment either:

- with the Variation Form, where the Supplier requests the Variation
- within the time limits included in a Variation Form requested by CCS or the Buyer

24.3 If the Variation to a Contract cannot be agreed or resolved by the Parties, CCS or the Buyer can either:

- agree that the Contract continues without the Variation
- terminate the affected Contract, unless in the case of an Order Contract, the Supplier has already provided part or all of the provision of the Deliverables, or where the Supplier can show evidence of substantial work being carried out to provide them
- refer the Dispute to be resolved using Clause 34 (Resolving Disputes)

24.4 CCS and the Buyer are not required to accept a Variation request made by the Supplier.

24.5 If there is a General Change in Law, the Supplier must bear the risk of the change and is not entitled to ask for an increase to the DPS Pricing or the Charges.

24.6 If there is a Specific Change in Law or one is likely to happen during the Contract Period the Supplier must give CCS and the Buyer notice of the likely effects of the changes as soon as reasonably

practical. They must also say if they think any Variation is needed either to the Deliverables, DPS Pricing or a Contract and provide evidence:

- that the Supplier has kept costs as low as possible, including in Subcontractor costs
- of how it has affected the Supplier's costs

24.7 Any change in the DPS Pricing or relief from the Supplier's obligations because of a Specific Change in Law must be implemented using Clauses 24.1 to 24.4.

25. How to communicate about the contract

25.1 All notices under the Contract must be in writing and are considered effective on the Working Day of delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective when sent unless an error message is received.

25.2 Notices to CCS must be sent to the CCS Authorised Representative's address or email address indicated on the Platform.

25.3 Notices to the Buyer must be sent to the Buyer Authorised Representative's address or email address in the Order Form.

25.4 This Clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.

26. Dealing with claims

26.1 If a Beneficiary is notified of a Claim then it must notify the Indemnifier as soon as reasonably practical and no later than 10 Working Days.

26.2 At the Indemnifier's cost the Beneficiary must both:

- allow the Indemnifier to conduct all negotiations and proceedings to do with a Claim
- give the Indemnifier reasonable assistance with the claim if requested

26.3 The Beneficiary must not make admissions about the Claim without the prior written consent of the Indemnifier which can not be unreasonably withheld or delayed.

26.4 The Indemnifier must consider and defend the Claim diligently using competent legal advisors and in a way that doesn't damage the Beneficiary's reputation.

26.5 The Indemnifier must not settle or compromise any Claim without the Beneficiary's prior written consent which it must not unreasonably withhold or delay.

26.6 Each Beneficiary must take all reasonable steps to minimise and mitigate any losses that it suffers because of the Claim.

26.7 If the Indemnifier pays the Beneficiary money under an indemnity and the Beneficiary later recovers

money which is directly related to the Claim, the Beneficiary must immediately repay the Indemnifier the lesser of either:

- the sum recovered minus any legitimate amount spent by the Beneficiary when recovering this money
- the amount the Indemnifier paid the Beneficiary for the Claim

27. Preventing fraud, bribery and corruption

27.1 The Supplier must not during any Contract Period:

- commit a Prohibited Act or any other criminal offence in the Regulations 57(1) and 57(2)
- do or allow anything which would cause CCS or the Buyer, including any of their employees, consultants, contractors, Subcontractors or agents to breach any of the Relevant Requirements or incur any liability under them

27.2 The Supplier must during the Contract Period:

- create, maintain and enforce adequate policies and procedures to ensure it complies with the Relevant Requirements to prevent a Prohibited Act and require its Subcontractors to do the same
- keep full records to show it has complied with its obligations under Clause 27 and give copies to CCS or the Buyer on request
- if required by the Relevant Authority, within 20 Working Days of the Start Date of the relevant Contract, and then annually, certify in writing to the Relevant Authority, that they have complied with Clause 27, including compliance of Supplier Staff, and provide reasonable supporting evidence of this on request, including its policies and procedures

27.3 The Supplier must immediately notify CCS and the Buyer if it becomes aware of any breach of Clauses 27.1 or 27.2 or has any reason to think that it, or any of the Supplier Staff, has either:

- been investigated or prosecuted for an alleged Prohibited Act
- been debarred, suspended, proposed for suspension or debarment, or is otherwise ineligible to take part in procurement programmes or contracts because of a Prohibited Act by any government department or agency
- received a request or demand for any undue financial or other advantage of any kind related to a Contract
- suspected that any person or Party directly or indirectly related to a Contract has committed or attempted to commit a Prohibited Act

27.4 If the Supplier notifies CCS or the Buyer as required by Clause 27.3, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

27.5 In any notice the Supplier gives under Clause 27.4 it must specify the:

- Prohibited Act
- identity of the Party who it thinks has committed the Prohibited Act
- action it has decided to take

28. Equality, diversity and human rights

28.1 The Supplier must follow all applicable equality Law when they perform their obligations under the Contract, including:

- protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise
- any other requirements and instructions which CCS or the Buyer reasonably imposes related to equality Law

28.2 The Supplier must take all necessary steps, and inform CCS or the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on a Contract.

29. Health and safety

29.1 The Supplier must perform its obligations meeting the requirements of:

- all applicable Law regarding health and safety
- the Buyer's current health and safety policy while at the Buyer's Premises, as provided to the Supplier

29.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer Premises that relate to the performance of a Contract.

30. Environment

30.1 When working on Site the Supplier must perform its obligations under the Buyer's current Environmental Policy, which the Buyer must provide.

30.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's Environmental Policy.

31. Tax

31.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. CCS and the Buyer cannot terminate a Contract where the Supplier has not paid a minor tax or social security contribution.

31.2 Where the Charges payable under a Contract with the Buyer are or are likely to exceed £5 million at any point during the relevant Contract Period, and an Occasion of Tax Non-Compliance occurs, the Supplier must notify CCS and the Buyer of it within 5 Working Days including:

- the steps that the Supplier is taking to address the Occasion of Tax Non-Compliance and any mitigating factors that it considers relevant
- other information relating to the Occasion of Tax Non-Compliance that CCS and the Buyer may reasonably need

31.3 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under an Order Contract, the Supplier must both:

- comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions
- indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Contract Period in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff

31.4 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains the following requirements:

- the Buyer may, at any time during the Contract Period, request that the Worker provides information which demonstrates they comply with Clause 31.3, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding
- the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer
- the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with Clause 31.3 or confirms that the Worker is not complying with those requirements
- the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management

32. Conflict of interest

32.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual or potential Conflict of Interest.

32.2 The Supplier must promptly notify and provide details to CCS and each Buyer if a Conflict of Interest happens or is expected to happen.

32.3 CCS and each Buyer can terminate its Contract immediately by giving notice in writing to the Supplier or take any steps it thinks are necessary where there is or may be an actual or potential Conflict of Interest.

33. Reporting a breach of the contract

33.1 As soon as it is aware of it the Supplier and Supplier Staff must report to CCS or the Buyer any actual or suspected breach of:

- Law
- Clause 12.1
- Clauses 27 to 32

33.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in Clause 33.1 to the Buyer or a Prescribed Person.

34. Resolving disputes

34.1 If there is a Dispute, the senior representatives of the Parties who have authority to settle the Dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the Dispute.

34.2 If the Dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution (CEDR) Model Mediation Procedure current at the time of the Dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the Dispute, the Dispute must be resolved using Clauses 34.3 to 34.5.

34.3 Unless the Relevant Authority refers the Dispute to arbitration using Clause 34.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:

- determine the Dispute
- grant interim remedies
- grant any other provisional or protective relief

34.4 The Supplier agrees that the Relevant Authority has the exclusive right to refer any Dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the Dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.

34.5 The Relevant Authority has the right to refer a Dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under Clause 34.3, unless the Relevant Authority has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under Clause 34.4.

34.6 The Supplier cannot suspend the performance of a Contract during any Dispute.

35. Which law applies

This Contract and any issues arising out of, or connected to it, are governed by English law.

36. Buyer Premises

36.1 Licence to occupy Buyer Premises

36.1.1. Any Buyer Premises shall be made available to the Supplier on a non-exclusive licence basis free of charge and shall be used by the Supplier solely for the purpose of performing its obligations under this Order Contract. The Supplier shall have the use of such Buyer Premises as licensee and shall vacate the same immediately upon completion, termination, expiry or abandonment of this Order Contract.

36.1.2. The Supplier shall limit access to the Buyer Premises to such Supplier Staff as is necessary to enable it to perform its obligations under this Order Contract and the Supplier shall co-operate (and ensure that the Supplier Staff co-operate) with such other persons working concurrently on such Buyer Premises as the Buyer may reasonably request.

36.1.3. Save in relation to such actions identified by the Supplier in accordance with paragraph 3.2 of Order Schedule 6 (where used) and set out in the Order Form (or elsewhere in the relevant Order Contract), should the Supplier require modifications to the Buyer Premises, such modifications shall be subject to Approval and shall be carried out by the Buyer at the Supplier's expense. The Buyer shall undertake any modification work which it approves pursuant to this Clause 36.1.3 without undue delay. Ownership of such modifications shall rest with the Buyer.

36.1.4. The Supplier shall observe and comply with such rules and regulations as may be in force at any time for the use of such Buyer Premises and conduct of personnel at the Buyer Premises as determined by the Buyer, and the Supplier shall pay for the full cost of making good any damage caused by the Supplier Staff other than fair wear and tear. For the avoidance of doubt, damage includes without limitation damage to the fabric of the buildings, plant, fixed equipment or fittings therein.

36.1.5. The Parties agree that there is no intention on the part of the Buyer to create a tenancy of any nature whatsoever in favour of the Supplier or the Supplier Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the relevant Order Contract, the Buyer retains the right at any time to use any Buyer Premises in any manner it sees fit.

36.2 Security of Buyer Premises

36.2.1 The Buyer shall be responsible for maintaining the security of the Buyer Premises. The Supplier shall comply with the reasonable security requirements of the Buyer while on the Buyer Premises.

36.2.2 The Buyer shall afford the Supplier upon Approval (the decision to Approve or not will not be unreasonably withheld or delayed) an opportunity to inspect its physical security arrangements.

37. Buyer Property

37.1 Where the Buyer issues Buyer Property free of charge to the Supplier such Buyer Property shall be and remain the property of the Buyer and the Supplier irrevocably licences the Buyer and its agents to enter upon any premises of the Supplier during normal business hours on reasonable notice to recover any such Buyer Property.

37.2 The Supplier shall not in any circumstances have a lien or any other interest on the Buyer Property and at all times the Supplier shall possess the Buyer Property as fiduciary agent and bailee of the Buyer.

37.3 The Supplier shall take all reasonable steps to ensure that the title of the Buyer to the Buyer Property and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Buyer's request, store the Buyer Property separately and securely and ensure that it is clearly identifiable as belonging to the Buyer.

37.4 The Buyer Property shall be deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Buyer otherwise within five (5) Working Days of receipt.

37.5 The Supplier shall maintain the Buyer Property in good order and condition (excluding fair wear and tear) and shall use the Buyer Property solely in connection with the relevant Order Contract and for no other purpose without Approval.

37.6 The Supplier shall ensure the security of all the Buyer Property whilst in its possession, either on the Sites or elsewhere during the supply of the Services, in accordance Order Schedule 9 (Security) and the Buyer's reasonable security requirements from time to time.

37.7 The Supplier shall be liable for all loss of, or damage to the Buyer Property, (excluding fair wear and tear), unless such loss or damage was solely caused by a Buyer Cause. The Supplier shall inform the Buyer immediately of becoming aware of any defects appearing in or losses or damage occurring to the Buyer Property.

38. Buyer Equipment

38.1 Unless otherwise stated in the relevant Order Contract, the Supplier shall provide all the Supplier Equipment necessary for the provision of the Services.

38.2 The Supplier shall not deliver any Supplier Equipment nor begin any work on the Buyer Premises without obtaining Approval.

38.3 The Supplier shall be solely responsible for the cost of carriage of the Supplier Equipment to the Sites and/or any Buyer Premises, including its off-loading, removal of all packaging and all other associated costs. Likewise on the Contract Expiry Date the Supplier shall be responsible for the removal of all relevant Supplier Equipment from the Sites and/or any Buyer Premises, including the cost of packing, carriage and making good the Sites and/or the Buyer Premises following removal.

38.4 All the Supplier's property, including Supplier Equipment, shall remain at the sole risk and responsibility of the Supplier, except that the Buyer shall be liable for loss of or damage to any of the Supplier's property located on Buyer Premises which is due to the negligent act or omission of the Buyer.

38.5 Subject to any express provision of the BCDR Plan (if applicable) to the contrary, the loss or destruction for any reason of any Supplier Equipment shall not relieve the Supplier of its obligation to supply the Services in accordance with this Order Contract, including the Service Levels.

38.6 The Supplier shall maintain all Supplier Equipment within the Sites and/or the Buyer Premises in a safe, serviceable and clean condition.

38.7 The Supplier shall, at the Buyer's written request, at its own expense and as soon as reasonably practicable:

38.7.1 Remove from the Buyer Premises any Supplier Equipment or any component part of Supplier Equipment which in the reasonable opinion of the Buyer is either hazardous, noxious or not in accordance with the Order Contract; and

38.7.2 Replace such Supplier Equipment or component part of Supplier Equipment with a suitable substitute item of Supplier Equipment.

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 S149 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 or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences 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 offences 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 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 that all workers are 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 ensure 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 is used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

5.3.1 this is allowed by national law;

5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and

5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

6. Sustainability

6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs