DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	Contract ref: C353518
THE BUYER:	**NHS England**
BUYER ADDRESS	**7-8 Wellington Place, Leeds, LS1 4AP**
THE SUPPLIER:	**MTI Technology Limited**
SUPPLIER ADDRESS:	**C/O Kpmg Llp Saltire Court, 20 Castle Terrace, Edinburgh, Scotland, Scotland, EH1 2EG**
REGISTRATION NUMBER:	SC112019
DUNS NUMBER:	399745017

DPS SUPPLIER REGISTRATION SERVICE ID: N/A

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 07th April 2025. It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Technical Remediation Services.

DPS FILTER CATEGORY(IES):
NCSC Assured Services, IT Health Check, Cyber Essentials Plus, Clearance: Security Check, ISO 27001, Government, Health

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 A
  - Order Schedule 10 (Exit Management)
  - Order Schedule 15 (Order Contract Management)
  - Order Schedule 20 (Order Specification)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6 -Not used
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

No other Supplier terms are part of the 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:

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, and following any termination or expiry of the Contract shall continue to comply, 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, and following any termination or expiry of the Contract shall continue to comply, 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) [HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);]

(e) ISO/IEC27001 and ISO/IEC27002.

3.6 The Supplier warrants and represents that for any system which holds any protectively marked Government Data it shall comply throughout the term, and following any termination or expiry of the Contract shall continue to comply 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)

An additional bullet shall be added to **Clause 9.1 (Intellectual Property Rights), and clause 9.2 shall be varied** as follows:

"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:

- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier
- develop and provide products and services to third parties."

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. The Supplier may at any time request 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 such terms as the Buyer may set, such request will not unreasonably be withheld. The Supplier acknowledges that where any such request relates to New IPR associated with data, that the Buyer may be restricted by reasons of applicable Law and contract. Nothing in this Contract shall be interpreted as the provision of permission by the Buyer to use Government Data or any New IPR derived from Government Data to develop or train AI or machine learning systems."

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 – Clause 19 (The Rights of Third Parties)

Clause 19 (Other people's rights in a contract) of the Core Terms shall be deleted and replaced with the following:

19.1 Subject to Clause 19.2, 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.

19.2 Where the Buyer either procures the Deliverables on behalf of, or to be provided to, a third party (such third party being a **Relevant Organisation** for the purposes of this Order Contract), the following shall apply:

19.2.1 the Relevant Organisation(s) may enforce the rights and obligations under this Order Contract; and/or

19.2.2 (without double counting) any Loss suffered or incurred by a Relevant Organisation due to a breach of the Supplier's obligations under this Order Contract shall be deemed to be a Loss of the Buyer, and the Buyer shall be able to recover the same under and in accordance with the terms of this Order 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)- Not Used

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 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. The/Both plan[s] will protect all aspects and processes associated with the delivery of the Services.

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

ORDER START DATE: 22nd April 2025

ORDER EXPIRY DATE: 21st April 2027

ORDER INITIAL PERIOD: 2 Years

ORDER OPTIONAL EXTENSION 1 Year

DELIVERABLES

The scope for Technical Remediation Services is predefined as per the requirements included in the tender and will be aligned to Order Schedule 20 (Order Specification).

An individual Work Order/fulfilment request will be requested by Health Organisations and passed onto the supplier via a Service Now request. The Parties acknowledge that these requests are not fully defined in terms of a standard catalogue request or bespoke remediation services, nor the requesting Health Organisation party in advance and at the point of awarding this Order Form and will be developed over the Contract Period as future requests are required ("**Future Services**"). Future Services will be called off using the Commissioning Process outlined at Appendix 1 to this Order Form.

The Buyer is not obliged to request any Future Services. In the event that the Buyer does raise a request for Future Services, the Supplier is required to respond in accordance with the Commissioning Process outlined in Appendix 1 to this Order Form.

"**Work Order**" means the detailed plan, agreed in accordance with Appendix 1 of this Order Form, describing the Services and/ or Deliverables to be provided by the Supplier, the timetable for their performance and the related matters listed in the

template Work Order set out in Appendix 1 of the Order Form. This will form part of future SOW's delivered under this contract.

LOCATION
The location of the Services will be carried out remotely or at a specified UK based location that will be confirmed at the time of instruction of a check requested.

Various locations will be supplied to the successful supplier as part of initiation activities. If unable to carry out onsite activities these will be done remotely in a secure manner using NCSC guidance**.**

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] in the first 12 months of the Contract. This is subject to budget/planning approval.

ORDER CHARGES
See details in Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD
Monthly in arrears upon completed deliverables

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]

7-8 Wellington Place, Leeds, LS1 4AP

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]
C/O Kpmg Llp Saltire Court, 20 Castle Terrace, Edinburgh, Scotland, Scotland, EH1 2EG

SUPPLIER'S CONTRACT MANAGER
[redacted]
C/O Kpmg Llp Saltire Court, 20 Castle Terrace, Edinburgh, Scotland, Scotland, EH1 2EG

PROGRESS REPORT FREQUENCY
Quarterly review meetings and annual reporting

PROGRESS MEETING FREQUENCY
Quarterly review meetings

KEY STAFF
[redacted]
C/O Kpmg Llp Saltire Court, 20 Castle Terrace, Edinburgh, Scotland, Scotland, EH1 2EG

KEY SUBCONTRACTOR(S)
The below subcontractors are named under this contract in support of the delivery:
[redacted]

[redacted]

COMMERCIALLY SENSITIVE INFORMATION
Refer to DPS Joint Schedule 4 Supplier's 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)

For and on behalf of the Supplier

[redacted]

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 17/04/2025

For and on behalf of the Buyer:

[redacted]

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 25/04/25

Annex 1- Work Order Process (request fulfilment)

Appendix 1 – Work Order Process (request fulfilment) - This Work Order should be read in conjunction with the terms of the Call-Off Contract between the parties dated [insert date when known] and the terms of the Call-Off Contract form part of this Work Order including but not limited to any limitations of liability therein.

i. Technical remediation requests are received as and when internal team's (Health and Care Organisations) requirement arises. Requests come into NHS England via our in-house system ServiceNow.
ii. The request is reviewed initially by the Cyber Operations team and once it is deemed sufficient in detail to share and within scope, the Cyber Operations will issue the new request to the supplier that is appointed the contract using ServiceNow.
iii. The supplier will manage all aspects of the customer onboarding from this point through to completion of the delivery. This will consist of
iv. Reaching out to the customer within two business days to arrange an onboarding call. This call will set out the expectations with the recipient organisation including resource commitment, data needed to run the tests, and devices they may need to setup to run cyber tests.
v. The supplier needs to keep the recipient organisation informed of progress, and highlight any critical issues found immediately
vi. Hold a close out call / debrief with the recipient organisation to discuss findings and recommendations how to correct issues found.
vii. The supplier will provide the outputs of each work order will be provided to recipient organisation and stored on NHSE SharePoint location. If any output contains personal data, this must be removed before they are provided to NHS England. If the report contains sensitive

data (e.g., IP address details) this should be redacted in the version of the report being sent to NHS England.

viii. The supplier will complete reporting as per an agreed format

ix. The supplier should notify the Cyber Operations team that the work is completed so the request can be closed within the ServiceNow toolset

Amendments to Work Orders (and associated pricing) after the execution of the associated Work Order shall follow the Variation process set out at in the Joint Schedules for RM3764iii Joint Schedule 2 (Variation Form).

The Order Contract is non-exclusive, and the Authority does not commit to awarding any work as part of this Contract.

Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

Contract Details		
This variation is between:	**[delete** as applicable: CCS / Buyer**]** (**"CCS" "the Buyer"**) And **[insert** name of Supplier**]** (**"the Supplier"**)	
Contract name:	**[insert** name of contract to be changed] **("the Contract")**	
Contract reference number:	**[insert** contract reference number]	
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 [redacted]

Date .....

Name (in Capitals) .....

Address .....

Full Name: [redacted]

Job Title/Role: [redacted]

Date Signed: 17/04/2025

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 one million pounds (£1,000,000);

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 five million pounds (£5,000,000); 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 five million pounds (£5,000,000).

Joint Schedule 4 (Commercially Sensitive Information)

1. What is the Commercially Sensitive Information?

1.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2 Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

No.	Date	Item(s)	Duration of Confidentiality
1	15/04/2025	Commercially Sensitive information	Duration of the contract

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 - MTI	[redacted]	[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.

The contact details of the Relevant Authority's Data Protection Officer are: Jon Moore - nhsdigital.dpo@nhs.net

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

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

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

1.4 For the avoidance of doubt, access to personal data is not expected to be generally necessary for the scope of the Services outlined in the Work Order under this Contract and the Order Form, and the Supplier Personnel shall not generally have access to any personal data of NHS England.

The Service Recipient (e.g. NHS Trust, Health Organisations) will be the Data Controller and the Supplier, who is determined as part of NHS England procurement, will be the Data Processor.
All personal data will be removed from the reports before these are shared with NHS England who therefore will not be a Data Processor or Controller for any of the data contained in the reports. NHS England as the Managed Security Service Provider (MSSP) only collect limited personal data of the contact details (name, email address, telephone number) of authorised staff in NHS organisations who onboard to the TR in order to provide this information to the supplier.

However, it is recognised that on occasion it may become necessary for NHS England to require services associated, where the Supplier will be given access to personal data. Where any such service request gives access to personal data, the Supplier shall access such data as processor to NHS England, and the following table shall apply (as updated where necessary in the agreed Work Order).

Description	Details
Identity of Controller for each Category of Personal Data	The Service Recipient (e.g. NHS Trust) will be the Data Controller and the Supplier, who is determined as part of NHS England procurement, will be the Data Processor.

Duration of the Processing	For the duration of this Order Contract and Work Orders arising hereunder. For the duration that the outcome reports are required for annual reporting.
Nature and purposes of the Processing	*All personal data will be removed from the reports before these are shared with NHS England who therefore will not be a Data Processor or Controller for any of the data contained in the reports. NHS England as the Managed Security Service Provider (MSSP) only collect limited personal data of the contact details (name, email address, telephone number) of authorised staff in NHS organisations who onboard to the TR Services in order to provide this information to the supplier.* *It is the Service Recipient's responsibility as to whether they would also choose to have a Data Processing Agreement between themselves and the Supplier* The types of data that may be collected by the Supplier on behalf of the Service Recipient to perform the Techincal Remediation Services include: - Staff data (NHS contact and work details to onboard) - Network data (Test against internet and N3 facing IT devices) - Patient Administration Data (account management, audit logs, server segregation, folder configuration and database setup) - File share data (types of access, any simple passwords in use and any back-up files on shares) - Active Directory data (password complexity, account lockout attempts, audit logs) - Antivirus data (centrally managed and no alerts urgent older than 2 days) - Patching data (centrally managed and applied within 3 months) - Backup data (adequate back-ups in place with restore tests in place) - Mobile device data (under MDM solution, encrypted, auto updated and password complexity) - Workstation data (checks for admin access, disk encryption, OS patches, USB usage, plug-ins for browsers etc.) The data is collected by the supplier using various techniques that will include interviewing and checks against system and configuration logs

	The Supplier must deliver final reports and recommendations in writing for each Technical Remediation workpackage Service to NHS England and to the assessed Health and Care Organisation. NHS England's version of the reports will have any IP address details redacted. The reports are: • *DSPT report showing key technical assurance and a RAG score to show if evidence was correct and comments against this.* • *Management summary and TR report capturing output activities and recommendations around how to take corrective actions, identifying the urgency of taking corrective actions based on a recognisable approach (e.g. RAG)* • *An NHS England summary report showing a holistic overview of DSPT and TR findings (RAG) to support internal NHS England reports.* *Further to the above reports, the supplier will be expected to complete a service delivery tracker created by NHS England to support invoicing and payment.*
Type of Personal Data	The below is between NHS England and The Supplier Name Email Address (Work only) Mobile Phone Number / Device Number/ IMEI No (NHS & Care Address only)
Categories of Data Subject	*This will depend on the nature of the product/systems/ services being tested in the Work Order but could include, but not limited to,* *Customer, Supplier, Citizen, and Patient.*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member	*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.*

State law to preserve that type of data	

B) DPS Contract Personal Data Processing

Description	Details
Identity of Controller for each Category of Personal Data	**CCS is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor of the Personal Data recorded below
Duration of the Processing	Up to 7 years after the expiry or termination of the DPS Contract
Nature and purposes of the Processing	To facilitate the fulfilment of the Supplier's obligations arising under this DPS Contract including i. Ensuring effective communication between the Supplier and CSS ii. Maintaining full and accurate records of every Order Contract arising under the Framework Agreement in accordance with Core Terms Clause 15 (Record Keeping and Reporting)
Type of Personal Data	Includes: i. Contact details of, and communications with, CSS staff concerned with management of the DPS Contract ii. Contact details of, and communications with, Buyer staff concerned with award and management of Order Contracts awarded under the DPS Contract, iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract Contact details, and communications with Supplier staff concerned with management of the DPS Contract

Categories of Data Subject	Includes: i. CSS staff concerned with management of the DPS Contract ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the DPS Contract iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract Supplier staff concerned with fulfilment of the Supplier's obligations arising under this DPS Contract
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	All relevant data to be deleted 7 years after the expiry or termination of this DPS Contract unless longer retention is required by Law or the terms of any Order Contract arising hereunder

Annex 2 - Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2-15 of Joint Schedule 11 (Where one Party is Controller and the other Party is Processor) and paragraphs 7-27 of Joint Schedule 11 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Relevant Authority]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Relevant Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Law as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Relevant Authority each undertake that they shall:

(a) report to the other Party every [x] months on:

(i) the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject before disclosing or transferring the Personal Data to the third partry. For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 2 (Data Sharing Agreement) and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(i) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Law, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Law and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Law to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. **Data Protection Breach**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming

aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. **Audit**

4.1 The Supplier shall permit:

(a) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, to conduct, at the Relevant Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Law; and/or

(b) the Relevant Authority, or a third-party auditor acting under the Relevant Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Relevant Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 GDPR.

6. ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

7.1 If financial penalties are imposed by the Information Commissioner on either the Relevant Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the Information Commissioner, the Relevant Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Relevant Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Relevant Authority, then the Relevant Authority shall be responsible for the payment of such Financial Penalties. In this case, the Relevant Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Relevant Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Relevant Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Relevant Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner, then the Relevant Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Clause 34 of the Core Terms (*Resolving disputes*).

7.2 If either the Relevant Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

(a) if the Relevant Authority is responsible for the relevant Personal Data Breach, then the Relevant Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Relevant Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Relevant Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Relevant Authority.

8. Termination

If the Supplier is in material Default under any of its obligations under this Annex 2 (*Joint Control Memorandum of Understanding*), the Relevant Authority shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 10 (*Ending the contract*).

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Law.

10. Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Law and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Law and its privacy policy.

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 Management	Contract Review Meetings	As required	Quarterly
Order Contract Charges	Rate card applied and discussed at SOW level	As required	At SOW level
Key Subcontractors	Advise if any changes	In writing to The Authority to process a variation	As and when an amend is required.

Order Schedule 4 (Order Tender)

[redacted]

Order Schedule 5 (Pricing Details)

Costs submitted as part of the tender bid form the costs associated with contract delivery when utilising the call-off procedure for Statement of Works or any deliverables relating to the contract for the lifetime of the contract.

Rate Card

The below rates are aligned to government industry standards with role and skill profiles to provide relevant requirements. These rates are utilised to form catalogue pricing for requirements related to Technical Remediation Services.

Vulnerability Management Principal- Daily Rate- [redacted]

Skil/Role Definitions- The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those

vulnerabilities and advise on implementing them

Lead complex information systems to understand and prioritise actions on Cyber Security risks, audit requirements and data value, and provide specialist or complex

guidance to vulnerability management teams and external senior stakeholders

• Lead the development and implementation of multiple vulnerability assessments and enterprise-wide scanning strategies across multiple complex environments, while leading

in prioritising those vulnerabilities through a risk-based approach

• Lead the triage of vulnerabilities, ensuring mitigation measures are implemented, and oversee the life cycle of vulnerability management for a set of assets, providing tailored

specialist or complex advice on ways to improve control mechanisms and mitigate risks

• Lead senior stakeholder engagement across government to create strategic plans for managing vulnerabilities and remediation activities

• Create organisational principles and vision that will provide the basis for triaging vulnerabilities

• Provide advice to senior leadership on ways to improve control mechanisms, identify, evaluate, and mitigate risks

• Develop bespoke templates and test scripts to meet uncommon or complex organisational objectives

• Set the organisation's vulnerability management strategy including people, process and technology elements

• Ensure organisation-specific vulnerability management policies, procedures and guidelines are aligned with organisational objectives and risk appetite

• Set direction and approve investment in strategic tooling and capability to address strategic enterprise-wide risk

• Develop bespoke templates and test scripts to meet uncommon or complex organisational objectives

Vulnerability Management Lead-Daily Rate- £[redacted]

Skil/Role Definitions- The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those

vulnerabilities and advise on implementing them

• Manage complex information systems to understand and prioritise actions on Cyber Security risks, audit requirements and data value, and provide guidance to vulnerability

management team members

• Manage the creation and implementation and lead development of vulnerability assessments for IT estates, including but not limited to application vulnerability assessments

and infrastructure vulnerability assessments

• Drive prioritisation of those vulnerabilities through a risk-based approach, to meet common organisational objectives such as regulatory compliance and audit functions

• Manage the triage of vulnerabilities, ensuring mitigation measures are implemented, and managing the life cycle of vulnerability management for a set of assets, providing

tailored advice on ways to improve control mechanisms and mitigate risks

• Recommend remediation strategies and provide advice on complex configuration changes in support of vulnerability remediation

• Proactively identify and leverage threat intelligence sources to inform strategic vulnerability mitigation measures

• Manage collaboration with stakeholders to create tactical plans relating to managing vulnerabilities, and oversee subsequent activities

• Demonstrate developed knowledge and understanding of approaches and tooling for performing vulnerability assessment against large and complex infrastructure

• Validate system configuration across multiple and complex interlinking systems

• Translate vulnerability management standards and best practice into organisation-specific policies, procedures and guidelines and champion standards and best practice

outside security functions

• Explain the need for effective vulnerability management processes and implications of poor performances

• Lead development and implementation of effective vulnerability management programs across the enterprise to meet organisational and regulatory and compliance requirements

• Develop vulnerability assessment templates and test scripts to meet common organisational objectives such as regulatory compliance and internal audit functions

Vulnerability Management Associate- Daily Rate- £[redacted]

Skill/Role Definition- The role of Vulnerability Management is to triage vulnerabilities by relevance and criticality to the organisation. Vulnerability Management then identify mitigations for those

vulnerabilities and advise on implementing them.

• Analyse complex information systems to understand the associated Cyber Security risks, audit requirements, and data value

• Support the creation and implementation of vulnerability assessments of enterprise assets to a predefined scope and schedule using predetermined templates and test

scripts, including but not limited to:

• application vulnerability assessments

• infrastructure vulnerability assessments

• Assist in the prioritisation of those vulnerabilities through a risk-based approach

• Triage and prioritise vulnerabilities, implement mitigating measures, and support in the life cycle of vulnerability management, providing standardised advice on ways to

improve control mechanisms and mitigate risk

• Collaborate with stakeholders to manage vulnerabilities and undertake remediation activities

• Communicate common mitigation strategies such as patching and basic configuration change (system hardening)

• Understand how local protective security measures can be applied to reduce vulnerability exposure

• Demonstrate knowledge of common approaches and tooling to perform vulnerability assessment and to validate system configuration

• Perform vulnerability assessments of enterprise assets with limited supervision to a predefined scope and schedule using predetermined templates and test scripts

• Develop and implement schedules for performing vulnerability assessments to meet organisational objectives and compliance requirement

Catalogue Costs

The below are costs for catalogue items that will be utilised to form part of the Statement of Works Call-Off during the lifetime of the contract.

Annex-1	Activity	Resource	Effort	Rate	Total Cost
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Annex-2	Activity	Resource	Effort	Rate	Total Cost
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Annex-3	Activity *	Resource	Effort	Rate	Total Cost
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Annex-4	Activity	Resource	Effort	Rate	Total Cost
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Annex-5	Activity	Resource	Effort	Rate	Total Cost
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Annex-6	Activity	Resource	Effort	Rate	Total Cost
[redacted]					

Annex-7	Activity	Resource	Effort	Rate	Total Cost
[redacted]					

Annex-8	Activity	Resource	Effort	Rate	Total Cost
[redacted]					

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

Non-COTS Third Party Software Licensing Terms-NOT USED

ANNEX B

COTS Licensing Terms-NOT USED

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 1 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
Account Director	[redacted]	[redacted]
Programme Manager	[redacted]	[redacted]
PMO Lead	[redacted]	[redacted]
Security Lead	[redacted]	[redacted]
Commercial Lead	[redacted]	[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 A applies

Part A: Short 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"	the occurrence of: a) any unauthorised access to or use of the 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 Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time;

2. Complying with security requirements and updates to them

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 Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer as part of its Order Procedure it shall also comply with the Security Policy and shall

ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 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 security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 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.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

(a) comply with the principles of security set out in Paragraph 4.2 and any other provisions of this Contract relevant to security;

(b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

(c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites 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;

(d) 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, 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;

(e) 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 provision of the Goods and/or Services and shall 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 Contract;

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

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

4.3 Development of the Security Management Plan

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will 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 its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer 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.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 Amendment of the Security Management Plan

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

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Deliverables and/or associated processes;

(c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

(d) any new perceived or changed security threats; and

(e) any reasonable change in requirements requested by the Buyer.

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

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the 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.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 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 to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent an equivalent breach in the future exploiting the same cause failure; and

(d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 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 Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

~~Part B: Long Form Security Requirements- Not Used~~

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 ~~[insert security representative of the Buyer]~~

2.3.2 ~~[insert 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 nnex 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

Not Applicable

Security Management Plan

NHS England
Security Policy.pdf

Information Security Policy

NHS England

Information Security Policy

Version number & Status	**2.3**
First published:	01/09/2020
Date updated:	01/08/2022
Next review date:	Annual Review- following NHSE Re-organisation
Policy prepared by:	[redacted]
Policy Owner:	[redacted]
Policy approved by and Date:	*30/03/2023:* [redacted]
Brief summary of changes since previous version:	*01/08/2022: Updates to current structure of NHS England and ways of working*

Contents

1. Purpose

NHS England are public bodies, with information processing as a fundamental part of their purpose. It is important therefore that NHS England's have a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

The purpose of NHS England's Information Security Policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but perhaps more crucially it encompasses the behaviour of the people who manage information in the line of NHS England business.

Information security is about peoples' behaviours in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that NHS England is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on NHS England business.
- A strengthened position in the event of any legal action that may be taken against NHS England (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified, and appropriate controls are implemented and documented.

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by NHS England by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and Information Governance policies.
- Working with other Arm's Length Bodies (ALBs) who share a common Open Service supply partner, to develop collaborative approaches, systems and processes relating to information security.
- Describing the principles of security and explaining how they are implemented in NHS England. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within NHS England a level of awareness of the need for information security as an integral part of day-to-day business.
- Protecting information assets under the control of NHS England.

Confidentiality	Access to data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time, when it is needed.

2. Scope

Staff of the following NHS England areas are within the scope of this document:

- Staff working in or on behalf of NHS England (this includes contractors, temporary staff, embedded staff, secondees and all permanent employees) and hosted bodies.
- NHS England's Commissioning Support Units.

3. Policy Statement

3.1 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions and descriptions.

Where the need may arise, a review of the employment contract may be taken with mutual agreement to include further security checks and access as per the staff job role.

Security requirements are subject to review and therefore staff will be made aware of any such changes where required.

3.2 Security Control of Assets

NHS England Corporate IT has established an IT asset management process and associated system; where applicable this will involve support and collaboration from any external vendor or service provider e.g., Advance365, OpenService etc.

All IT assets, (hardware, software, application, or data) shall have a named Information Asset Owner who shall be responsible for the information security of that asset.

IT asset registers will be stored by the respective service providers with access and/or updated copies of the registers provided to the IT team in the IT asset catalogue. All assets which contain personal information will be logged on the IAMS system.

3.3 Information Security Management System (ISMS)

An ISMS is a systematic approach to managing information so that it remains secure. The ISMS uses a risk-based approach to secure information by applying stringent checks and controls to human resources, processes, and IT systems.

Steps will be taken to align NHS England's information security and IT policies and procedures in line with industry standards and ISMS processes e.g., ISO27001.

The group responsible for this is the Information Security Management System Group. This group is chaired by the Deputy Director Infrastructure, Security, Corporate IT and Smarter Working and reports directly to the Director of Corporate IT and Smarter Working and to the SIRO.

3.4 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information, as approved by the relevant IAO. All access shall be monitored to ensure it is in line with the user's role and responsibilities and that there is no excess of access or access creep. This will be done by ongoing vigilance, users informing IT as part of the incident reporting process or annual audits for assurance purposes.

Though primarily access will be granted through Active Directory, other access control mechanisms including single sign-on shall be used and deployed.
3.4 to 4.0 applies for NHSE assets and not personal assets where our services are consumed. For personal devices accessing our services please refer to the Acceptable use of ICT Policy and the Use your own device policy.

3.5 Computer Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

3.6 Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

Access shall be reviewed and where necessary redacted when not required as part of a user's role.

3.7 Equipment Security

To minimise loss of, or damage to, all assets, the Corporate IT team shall ensure that all electronic equipment and assets shall be identified, registered and physically protected from threats and environmental hazards.

All devices must be kept secure, and their screens locked when not in use. In public areas, extra attention should be paid to ensure devices are not left unattended.

In the event of loss or theft of any mobile or portable device, it must be reported to the police and the crime reference number provided to the IT Service/Support Team.

3.8 Mobile/Portable Devices and media

Portable devices, for example, laptops must be encrypted and kept securely and their screen locked when not being used. In public areas extra attention should be paid to ensure devices are not left unattended. All use of removable media must be authorised by the member of staff's line manager, who must accept responsibility for any risk raised by the use of the removable media. This request must be endorsed by the Information Security Manager from a security perspective and maybe referred to the IG team if there are data protection concerns.

NHSE does not endorse the use of USB drives. We recommend that this data is stored on cloud hosted NHSE O365/Azure instance. Where this is not possible i.e. exceptional edge conditions, we recommend that only encrypted drives be used but only after getting approval from [redacted]

Corporate IT systems automatically encrypt removable media. Removable media (including USB flash media) that will be used by NHS England employees internally or externally requires approval. The users line manager must support the request explaining the business need and purpose. The request for approval will go to the Information Security team [redacted] before the media may be used on NHS England devices, the user's line manager must accept responsibility for any risks associated with its use. Users breaching this requirement will be subject to disciplinary action.

This applies to media provided by the corporate IT and procured by the teams themselves in line with IT security requirements for removable media.

3.9 Physical Security

The physical security of NHS England's information is the responsibility of all staff. The protection of both personal and non-personal information is paramount in maintaining confidentiality. The physical environment must be recognised as providing a layer of protection to data and information. This is achieved by the following means:

- Controlling access to sites, buildings and offices
- Ensuring desks and work areas are clear at the end of each day
- Use of locked cabinets within offices to restrict access to information
- Checking that visitors to sites are authorised to be there
- Ensuring that when information is taken off site, it is done so securely or preferably via a means of encryption
- Always wearing an ID badge when on site

Staff security requirements shall be addressed at the recruitment stage and

all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

3.10 Viruses, Malware and Malicious Code

All IT equipment used by staff is protected by countermeasures and management procedures to protect against the threat of malicious software. This includes an approved anti-virus (AV) software, intrusion detection and prevention software and hardware controls and suspicious email traffic blocking by NHSmail. The Corporate IT will ensure that all AV software is functioning correctly and is up to date with the latest virus definitions. All incoming and outgoing internet traffic will be routed through dedicated servers and other network devices that provide AV scanning.

All staff shall be expected to co-operate fully with this policy. Users shall not install software on NHS England's property without permission from the IT Service Desk ITservicedesk@england.nhs.uk

3.11 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of NHS England.

All changes will be actioned as per section 4.17 below.

3.12 Email

Access is granted to the internet and NHS mail primarily for legitimate business purposes. Limited and reasonable personal use is permissible. Each employing organisation and your NHS mail provider reserve the right in their absolute discretion to withdraw permission for personal use of the internet and/or email at any time. Personal use should take place substantially out of normal working hours.

Your NHS Mail account is provided as a business tool by NHS Digital. This policy also applies to any other email account in use for business purposes within NHS England.

This policy, together with the Acceptable Use of ICT and User Obligations Policy applies to the use of NHS mail accounts. In the event that you are absent for a substantial period of time, or where you are no longer employed and access to your mail account is required for business continuity purposes, such access may be granted where deemed necessary and proportionate following a Data Protection Impact Assessment, which must be sent to the Information Governance Team and only after approval from the Senior Information Risk Owner or Deputy and the Director or regional HR Director.

Emails marked as personal that are stored within your email accounts will only be accessed knowingly in exceptional circumstances and where it is proportionate in the circumstances i.e. an investigation is taking place.

NHS mail accounts belonging to staff leavers shall remain accessible for a period of 3 months; 6 months for inactive accounts. Access will only ever be provided to a third party after a Data Protection Impact Assessment has been undertaken. Access to archived emails can be sought but only in very exceptional circumstances.

NHS mail remains a non-NHS England service and thus we have limited administrative access around its use and backend processes.

Whilst using NHS mail, staff are required to agree and follow the terms of the NHS mail service as per their guidance documents available on their website.

3.13 Information Asset Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAOs shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Please see the Information Risk Procedures for further information.

3.14 Information Security Events and Weaknesses

All NHS England information security events, near misses, and suspected weaknesses are to be reported to the Information Security team- in the first instance. All adverse incidents shall be reported to the NHS England Information Governance Team also. For the purpose of reporting, the Information Security Incident Reporting procedures must be complied with.

3.15 Classification of Sensitive Information

NHS England shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection (DSP) Toolkit to secure their information assets. Further details of the classifications controls can be found in the Corporate Document and Records Management Policy.

3.16 Protection from Malicious Software

NHS England and its Corporate IT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on NHS England's property without the necessary appropriate permissions.

Users breaching this requirement may be subject to disciplinary action as they are putting NHS England's network, attached devices, users and the data which NHS England hold at risk.

3.17 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. NHS England will put in place routines to regularly audit compliance

with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for example:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

3.18 Access to locations where personal data is stored and processed

NHS England have documented physical access control policies and procedures in place for all restricted areas. We maintain a system of employee identification, verification and authorisation and generate security passes for sites and restricted areas.

Additionally, building pass management is undertaken by the Estates Management function, provided by the estate and facilities provider (e.g. DHSC).

Visitor sign-in registers are used in conjunction with temporary access passes to control access for non-employees to sites. Security guards are present at all sites. Key sensitive areas have additional coded locks or swipe card access restrictions, such as the server and communications rooms.

3.19 Accreditation of Information Systems

NHS England shall ensure that all information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the Information security team after technical review and presented at the Information Security Management System (ISMS) group meeting before they commence operation. All SLSPs should also be reviewed by Corporate IG should the system process personal data.

3.20 Systems Change Control

Changes to information systems, applications or networks shall be reviewed and submitted to the Change Advisory Board (CAB) for approval prior to change. In certain circumstances minor or routine changes may be approved by a senior manager after consulting with stakeholders and for urgent emergency changes.

3.21 Business Continuity and Disaster Recovery Plans

NHS England will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).

Business Impact Analyses will be undertaken in all areas of NHS England. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The Director of Corporate IT, Infrastructure and Smarter Working has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

The SIRO has overall accountability.

3.22 Risk and audit-based approach

All information assets must be risk assessed and identified risks recorded in the relevant IT/IG risk register, and escalated to the corporate risk register where required, with management approval. Action plans will subsequently be put in place to mitigate the identified risks. Any implemented information security arrangements will be reviewed on a regular basis by the risk owner, following up with spot checks by the Information Governance Assurance and Planning Team.

NHS England will ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

Any security measures must be viewed as necessary protection against a risk of an event occurring, or to reduce the impact of such an incident. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The threat of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- The impact that such a threat would have if it occurred.
- The likelihood of such a threat occurring.

Additional audits shall be conducted in line with organisational requirements for assurance of security controls, data protection and time to time directives.

Annual audits shall be listed in the information security audit planner. This includes annual penetration testing of all the NHS England internet facing URLs and IP ranges.

3.23 Data and Information backup

NHS England will ensure that data located on network servers is backed up in accordance with the approved network back-up procedure. The backup or restore procedures for all systems will include performing backups to a defined schedule for example, every 24 hours, at the end of each work period.

Such information is to be stored off-site as required to minimise the loss of information destroyed as a result of local building or system damage. Backups are to be checked and assessed for integrity on a regular basis.

Cloud backups are in line with contractual agreements with the cloud platform providers.

3.23.1 Security and storage of backups

All backup media will be securely stored, accounted for and will only be available to authorised persons. Where long term storage is required for regulatory or legislative compliance, care should be taken to ensure that the media on which the data is held will not become obsolete or degraded during the storage period.
The above applies to on-prem or physical backup solutions where applicable.

3.23.2 Data Retention

NHS England holds and processes a significant amount of data of several types. These different data types additionally have different retention periods which are detailed in the Corporate Records Retention Schedule.

Records should be reviewed regularly to ensure that retention guidelines are being adhered to. If staff have any queries, they should contact england.ig-corporate@nhs.net .

3.24 Human Resource Security

NHS England will ensure that employees and third-party users understand their responsibilities and that their system access is suitable for their roles. Security responsibilities shall form part of their contract and induction.

All candidates shall be screened in relation to the sensitivity of their considered role.
For the duration of their contract all HR disciplinary processes shall be applied to cases of employees committing serious security breaches.

Upon termination of employment, contract or agreement, all employees are required to return all information assets in their possession back to NHS England as per the Leaver's Policy. Additionally the access rights of all employees, contractors and third-party users to information and information processing facilities will be removed on termination of employment, contract or agreement, or adjusted as necessary on change of role.

3.25 Security of external parties

NHS England will assign access to third party organisations based on a risk assessment. This will ensure that access is only granted where there is a genuine, authorised business need. The security of NHS England assets may be put at risk by third parties if they do not have the correct security controls in place. The risk assessment shall aim to identify such risks and mitigate against them.
All contracts should include schedules for escalation of cyber incidents to NHS England without delay and annual re-assertion to NHS England's cyber requirements.

3.25.1 Third party contracts

All third party contracts must be reviewed and the necessary information governance and information security requirements must reflect their acceptance of the Information Security Policy. Where third party service delivery is used to provide operational services to NHS England, security controls, service definitions and delivery levels should be specified in the relevant contracts and agreements. Services, reports and records from the third-party supplier should be regularly reviewed and monitored by the relevant lead/procuring manager supported by the Corporate IG team.

Audits of the services provided should be planned and conducted where practical and possible. The right to monitor, audit and revoke user access and third-party access is included in the contract clauses. Clauses to ensure the return and/or destruction of any NHS England information at the end of the contract must be present in addition to acceptance of any other NHS England policies and procedures relevant to the contract.

3.26 Information Disposal

Any equipment which holds, stores or processes data for NHS England or will be securely cleared or destroyed at the end of its functional life. Sensitive data, licensed software and other material will be securely erased or overwritten prior to releasing equipment for re-use or disposal. Computer assets must be disposed of in accordance with the IT asset disposal procedure and a Record of Disposal Certificate must be issued by the contracted disposal company.

All data storage devices must be purged of personal or commercially sensitive data before disposable. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider.

Printed matter containing sensitive information should be destroyed using an appropriate method, such as shredding or using confidential waste bins.

Working remotely, staff should ensure they dispose of such data in as secure a manner as possible. If you do have a shredder available, then best effort must be done to manually shred the documents to as small pieces as possible as you would your own personal information.

3.27 Training & Awareness

Training is mandatory and all staff are required to complete annual on-line IG training via the ESR system which includes data security and protection modules.

All guidance, policy, and awareness related documentation shall be available to all staff on the joint intranet for easy access and reference. Staff can also contact the information security team with any queries they may have at any time at [redacted] .

3.28 IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure must be complied with when:

- A new process is to be established that involves processing of personal data (data relating to individuals);
- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data;
- Introducing any new technology that uses or processes personal data in any way.

3.29 Use your own device (UYOD)

Please refer to the “Use your Own Device” policy.

4. Roles and Responsibilities

4.1 Chief Executive

Responsibility for information security resides ultimately with the Chief Executive. This responsibility is discharged through the designated roles of Senior Information Risk Owner and Deputy Director Infrastructure. Corporate IT and Smarter Working, as per business needs and Information Security industry best practice for governance,

4.2 Senior Information Risk Owner (SIRO)

The national Senior Information Risk Owner (SIRO) is responsible for information risk within NHS England and advises the Board on the effectiveness of information risk management across NHS England.

Deputy SIROs have also been appointed in central and regional teams to support the national SIRO.

Hosted bodies, including CSUs will have their own SIRO.

4.3 Data Protection Officer (DPO)

As a public authority NHS England are required to appoint a Data Protection Officer under the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in NHS England for data protection matters. The DPO reports to the SIRO and directly to the Board in relation to data protection matters.

CSUs have appointed Deputy DPOs that report directly to the joint NHS England DPO.

4.4 Senior Managers

As per this and associated policies, Senior Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures, and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.

4.5 Head of Corporate Information Governance (IG)

The Head of Corporate IG will be responsible for maintaining appropriate policies and guidance for staff around the use and processing of personal data or information contained within NHS England's 's information assets in line with data protection and data security legislation and regulations.

4.6 Deputy Director Infrastructure, Corporate IT and Smarter Working

The Deputy Director of Infrastructure, Corporate IT and Smarter Working is responsible for developing, implementing, and enforcing suitable and relevant information security procedures and protocols to ensure NHS England and its partner organisations systems and infrastructure remain compliant with relevant legislation, guidance, and security industry best practice.

They are responsible for ensuring the continuous review, update, and alignment of all IT assets as well as policies and procedures to conform to applicable guidance and security requirements.

4.7 Information Security Manager

The Information Security Manager will support the Deputy Director of Infrastructure, Corporate IT and Smarter Working to implement the above and lead on the operational information security processes and projects across NHS England and its subsidiary entities.

The Information Security Manager shall be the point of contact for all internal information security assurance, training, testing, developments, investigations, and queries.

4.8 Information Asset Owners (IAOs)

All IAOs are responsible for ensuring the confidentiality of their assets and maintaining up to date access lists of users. They must ensure that third-party data processors

have appropriate information security and/or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties.

IAOs are also responsible for ensuring appropriate data protection assurance from all third-party suppliers processing NHS England or data for their own information assets.

4.9 All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake their mandatory annual IG training and ensure that they also understand:

- What information they are using, how it should be protectively handled, stored, and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected beach of information security within NHS England.
- Their responsibility for raising any information security concerns with the Information Security Manager and reporting incidents directly through the online incident reporting portal.

4.10 External contractors

Contracts with external contractors that allow access to NHS England's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all our appropriate security policies.

Staff with additional 'administrative' accounts to systems are required to agree to additional undertakings regarding their enhanced level of responsibilities.

Contractors is defined as all NHSE staff who are not salaried via the NHS England Electronic Staff Record (ESR System).

5. Impact Assessments

5.1 Policy Impact Assessment

As part of the development of this policy, its impact on the business has been assessed; no detrimental issues were identified.

5.2 Equality and Health Inequality Analysis

As part of the development of this policy, its impact on equality has been analysed and no detriment identified.

6. Associated Documentation

The following documents will provide additional information:

- Acceptable Use of ICT and User Obligations
- Confidentiality Policy
- Document and Records Management Policy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Policy
- Information Sharing Policy

7. References – legislation

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012)

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 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

Scope of requirement

Standard Service catalogue – Discovery, over several years NHS England have been developing a set of standard work packages that is added to the service catalogue and made available to the organisation in scope to be consumed. This allows us to support local organisations centrally by funding targeted discovery packages to reduce risk.

The supplier must have proven and demonstrable skills and experience to provide different types of review/assessment work packages that are designed to cover a specific scope and will be repeatable and scalable across multiple recipient organisations. This will support recipient organisations in identifying security risks, highlight gaps between their infrastructure and best practice and provide remediation recommendations. The supplier should set out how they would deliver the following standard offerings

1. **Secure backup review** - An assessment of an organisations existing back-up and recovery solution to identify risks, measure alignment to NCSC guidelines and provide recommendations to secure back-ups. As detailed in Annex 1 – Secure backup review v1.0
2. **Secure backup reassessment** - Reassessment of a backup environment that was previously considered as being out of alignment following the completion of the backup review engagement, where trust have undertaken remediation activities and wish to be reassessed. As detailed in Annex 2 – Secure backup reassessment v1.0
3. **Active directory Security review** - An assessment of an organisations Active directory deployment, offering pragmatic mitigations that will increase its security and operational strength. As detailed in Annex 3 – Active directory security review v1.0
4. **Multi-factor authentication (MFA) Policy Gap Analysis and Planning** - Assess and track compliance with this national multi-factor authentication (MFA) policy and provide remediation action plans to enable Health and Social Care Organisations to implement relevant controls to comply

with the MFA policy. As detailed in Annex 4 – MFA policy gap analysis and planning v1.0

5. **Network Segmentation Review** –. Assess the level of maturity and the remediation actions that may be required for an organisations network to be aligned to the Network Segmentation Principles that have been published by NHS England in their Network segmentation. As detailed in Annex 5 – Network Segmentation review v1.0

6. **Vulnerability Management Maturity Assessment (VMMA)** -. Assess the recipient organisations Vulnerability Management Maturity covering people, process, and technology within the Governance, Risk and Compliance (GRC) to establish key areas of risk and provide recommendations for improvement. As detailed in Annex 6 – Vulnerability management maturity assessment (VMMA) v1.0

2. **Standard Service catalogue – Remediation**, in response to feedback from organisations advising they are having difficulty in remediating recommendations identified as part of the discovery work, NHS England have developed different types of remediation work packages that are designed to cover a specific scope, and which will be repeatable and scalable across multiple recipient organisations.

The supplier must have proven and demonstrable skills and experience to provide different types of remediation work packages that are designed to cover a specific scope and will be repeatable across multiple recipient organisations. These typically will involve the implementation, configuration and execution of solutions to execute security recommendations with a view to reduce cyber risk and comply with relevant data protection, cyber security standards and best practice. Supplier should set out how they would deliver the following standard offerings

1. **Role Based Authority (RBA) Accelerator** - Domain boundary - Implement a Role-based Authority architecture within the Active Directory to provide a significant increase in the granular provision of authorisation for administrative tasks. As detailed in Annex 7 – RBA Accelerator - Domain boundary v1.0

2. **Role Based Authority (RBA) Accelerator – Server zoning extension** - Implement a second security boundary into the Active Directory infrastructure that works in conjunction with the RBA and Domain Zone implemented in the previous

RBA Accelerator – domain boundary. As detailed in Annex 8 – RBA Accelerator – Server boundary extension v1.0

3. **Bespoke technical remediation** - A key activity undertaken by NHS England is to support local organisations to mitigate risk and build cyber resilience. This means that we need to provide targeted once-off support. Bespoke Technical Remediation allows organisations to request specialist support and expertise to scope and deliver once-off bespoke work packages to help organisations address vulnerabilities across their estate providing the request cannot be fulfilled by other means such as.

- Support is not available via an existing NHS England national service.
- Recipient organisation has not already received funding to address the risk / issue.
- The outcome will increase the recipient organisations cyber posture and resilience mitigating the risk of a Cyber-attack at the recipient organisations.

Typically, recipient organisations would have carried out standard service catalogue discovery and / or remediation service to highlight the need for further bespoke work, or alternatively the recipient organisation may already have evidence of vulnerabilities and risks from other forms of assessment delivered outside of the Technical Remediation programme which may require remediation support. The types of previous work covered included creation of operational policy, Process, Risk, Compliance, Strategy documentation as well as assessment and reconfiguration of existing technologies.

1. The capability of this aspect is aligned to the capacity of the selected supplier. Therefore, the supplier must demonstrate their capacity and ability to meet this requirement and provide evidence of their capabilities to support varying nature of IT across Health and Care.

Additionally, the following areas are considered a high priority, and supplier should set out how they would deliver the following bespoke requirements

2. **Active Directory remediation** – Describe how you would provide follow up support to resolve concerns that are identified through Active Directory security reviews. Your response should include:

1. Your approach to supporting an organisation with the remediation of the range of risks and issues that are commonly identified during Active Directory security reviews
2. Incorporation of transformation/innovation capabilities to uplift an organisation's Active Directory in line with best practice modern design as appropriate, for example through exploiting the capabilities centrally available as part of NHS Connect (formerly NHSmail) Shared Tenant Entra ID.

3. **Microsoft Extended Detection & Response support** - Authority is in the process of deploying Microsoft Extended Detection & Response across the NHS. Outline your approach to support the adoption / deployment of Microsoft Defender for Endpoint (MDE) (across all local compatible devices) and Microsoft Defender for Identity (MDI) (to local Domain Controllers). Your proposal should include your plans for providing:
   1. Hands-on technical support to NHS organisations
   2. Innovative promotion of the capabilities and benefits of the MDE/MDI services
   3. A methodology for supporting self-service deployment against recognised best practice.
4. **Extended Secure Backup support -** Over the past four years, Authority has undertaken 200 Secure Backup reviews to assess organisations in scope existing backup solution against National Cyber Security Centre 3:2:1 guideline (see Offline backups in an online world - NCSC.GOV.UK)). To support continual improvement in this area, please outline your approach to achieve the following objectives:
   1. Undertake a full security assessment of an organisation's backup solution, testing the existing security controls that are in place which aim to protect the organisations critical data against targeted attacks.
   2. Undertake an independent assessment of the organisations backup and restore capabilities for a critical system e.g. Trust Integration Engine (TIE). The aim is to assess a full restore test of the critical system in scope, that includes verification of data integrity, testing of recovery processes, assessing the achievability of Recovery point objective (RPO) and Recovery time objective (RTO) against business objectives etc.

5. If the authority deems there is demand for the targeted bespoke work package to be industrialised, then the work

package will be developed and added to the standard offering catalogue and offered more widely to the organisations in scope.

4. **Enhance the technical remediation service catalogue** - NHS England are always keen to enhance what we offer to the wider NHS system and in collaboration with the supplier actively look to innovate using data and industry knowledge. This may include reporting back to NHS England on key trends and findings from work undertaken and then providing innovative solutions to address these issues. This could cover but not limited to technical advice, guidance, development of standardised discovery and remediation support on specific emerging subject areas.

Utilising innovative techniques, the supplier should be proactive in the development of a more flexible portfolio that meets current and future customer's needs. Inputs into this activity may include lessons learned from work undertaken, stakeholder knowledge and expertise, industry best practise, our cyber strategy. The supplier must have proven, and demonstrable skills to provide these enhancements.

The key point about this element of the scope is that solutions are delivered in innovative ways, to allow scalable support to a large number of organisations. These offerings must maintain high quality outputs and deliver value for money. This type of support will be scoped with NHS England and the supplier when needed. The types of work undertaken to-date and expectation on the supplier to continue include, but not limited to the following:

1. Development of new discovery and remediation work packages and supporting collateral on specific subject areas.
2. Repurposing of the existing standard service catalogue to support smaller organisation types.
3. Best practice and technical guides - Detailed and step by step instructions for organisation to access and adapt to the local environment.
4. Best practice / technical videos - Instructional videos showing configuration in action for organisation to access and adapt to the local environment.
5. Webinars – Provide content and attendance to webinars covering key topics on current offerings to advertise and promote.

6. Documentation – this could include Architectural patterns, operational policies, strategy information that organisations can access and adopt locally.

5. **Out of scope**
   1. Technical remediation is service focussed and is not requiring the Supplier to offer hardware/software products to recipient organisations
   2. Out of hours support, all technical remediation services are expected to be to be delivered in core hours Monday to Friday 8-6

6. The requirement

The objective of the Call-off Contract is to provide the Buyer an appointment of a Supplier to work in partnership with to provide technical remediation services to support the Authority during the term of this Call-Off Contract.

1. **Standard Service catalogue – Discovery -** Aligned to Background to requirement/overview of requirement, section 3.3.1, and Scope of requirement, section 5.1
   1. Supplier will be responsible for receiving the service request from NHSE and working with the recipient organisation to onboard them and deliver on the predefined scope in accordance with an agreed statement of work.
   2. The supplier shall co-ordinate the work package with the recipient organisation to ensure the pre-requisites are understood and the correct personnel, materials and other preparatory activities are conducted.
   3. The supplier shall escalate to NHS England any challenges or concerns they have in delivering the agreed statement of work. This will be done through regular meeting or ad-hoc if urgent and documented via an issue log.
   4. The supplier shall produce a report for NHS England and each recipient organisation as an output work package
   5. Where applicable, the supplier shall recommend technical remediations and improvements in alignment with the latest version of the DSPT, NCSC guidelines, and industry best practice. Recommended remediation should consider a wide variety of options, to allow the recipient organisation to select its preferred IT methods and solutions.
   6. The supplier will notify NHSE England that the service request is now completed using the standard request fulfilment process.

7. The supplier will ensure the service delivery tracker (SDT) is updated with the correct detail so the invoice can be sent using the standard invoice process and approved.

2. **Standard Service catalogue - Remediation -** Aligned to Background to requirement/overview of requirement, section 3.3.1, and Scope of requirement, section 5.2

1. Supplier will be responsible for receiving the service request from NHSE and working with the recipient organisation to onboard them and deliver on the predefined scope in accordance with an agreed statement of work.
2. The supplier shall co-ordinate the work package with the recipient organisation to ensure the pre-requisites are understood and the correct personnel, materials and other preparatory activities are conducted.
3. The supplier shall escalate to NHS England any challenges or concerns they have in delivering the agreed statement of work. This will be done through regular meeting or ad-hoc if urgent and documented via an issue log.
4. The supplier shall produce a report for NHS England and each recipient organisation as an output work package
5. If applicable, the supplier shall recommend further technical remediations and improvements in alignment with the latest version of the DSPT, NCSC guidelines, and industry best practice. Recommended remediation should consider a wide variety of options, to allow the recipient organisation to select its preferred IT methods and solutions.
6. The supplier will notify NHSE England that the service request is now completed using the standard request fulfilment process.
7. The supplier will ensure the service delivery tracker (SDT) is updated with the correct detail so the invoice can be sent using the standard invoice process and approved

3. **Bespoke technical remediation -** Aligned to Background to requirement/overview of requirement, section 3.3.1, and Scope of requirement, section 5.3

1. Supplier will be responsible for receiving the service request from NHSE and working with the recipient organisation to onboard them to initially scope the requirements as per Work order process detailed in.
2. Appendix 2 – High level bespoke remediation scoping process & Statement of works requirements
3. Appendix 3 – Statement of works requirement.

4. Supplier will undertake documented activities against the agreed statement of work.
5. The supplier shall co-ordinate the work package with the recipient organisation to ensure the pre-requisites are understood and the correct personnel, materials and other preparatory activities are conducted.
6. The supplier shall produce a report for NHS England and the recipient organisation as an output.
7. Where applicable, the supplier shall recommend technical remediations and improvements in alignment with the latest version of the DSPT, NCSC guidelines, and industry best practice. Recommended remediation should consider a wide variety of options, to allow the recipient organisation to select its preferred IT methods and solutions.
8. The supplier will provide their thoughts around whether the work delivered can be standardised in a cost-effective manner and scaled-up to be delivered to the wider NHS.
9. The supplier shall escalate to NHS England any challenges or concerns they have in delivering the agreed statement of work. This will be done through regular meeting or ad-hoc if urgent and documented via an issue log.
10. The supplier will notify NHSE England that the service request is now completed using the standard request fulfilment process.
11. The supplier will ensure the service delivery tracker (SDT) is updated with the correct detail so the invoice can be sent using the standard invoice process and approved

4. **Enhance the technical remediation service catalogue -** Aligned to Background to requirement/overview of requirement, section 3.2.1, 3.3.2, and Scope of requirement, section 5.4

1. This type of support will be scoped with NHS England and the supplier when needed.
2. Mobilisation, supplier to support the authority to further specify of the scope, requirements, resources and delivery approach
3. Design, supplier to support the authority in the development of design options around the requirements based on user research and engagement. Further identify risks and change impact of proposed designs, as well as costing options
4. Build, supplier to build from options into viable solutions based on approved design, which are then tested with users via early adopters and iteratively improved

5. Implementation, supplier to support the transition to a standard operating model to scale up the service as the finalised product is made available for general consumption via the standard service catalogue (as described in sections 6.1 & 6.2)

7. Key milestones and deliverables

1. The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date
Kick off	An initial meeting between NHS England and Supplier for the purposes of • Introduction to the parties' teams • Additional information and context regarding the Authority's organisation • To further clarify the scope	Within week 1 of Contract Award
Mobilisation and onboarding	Collaboration to build artefacts and establish governance controls ahead of technical remediation services going live from 1st April 2025, including. • Onboarding supplier stakeholders • Development of artefacts and goverance to support the delivery of technical remediation • Development and sign off current standard service catalogue artefacts • Releasing backlog of requests / tickets for technical remediation	31st March 2025
FY 25/26 contract requirements	Statement of work detailing the authority requirements agreed with supplier	31st March 2025

FY 25/26 Contract Commitments	Complete technical remediation services in accordance with an agreed statement of work	31st March 2026
FY 25/26 Annual report	Complete an annual report detailing key trends and findings for each of the technical remediation services via an agreed format.	31st March 2026
FY 26/27 contract requirements	Statement of work detailing the authority requirements agreed with supplier	31st March 2026
FY 26/27 Contract Commitments	Complete technical remediation services in accordance with an agreed statement of work	31st March 2027
FY 26/27 Annual report	Complete an annual report detailing key trends and findings for each of the technical remediation services via an agreed format.	31st March 2027
FY 27/28 contract requirements *	Statement of work detailing the authority requirements agreed with supplier	31st March 2027
FY 27/28 Contract Commitments *	Complete technical remediation services in accordance with an agreed statement of work.	31st March 2028
FY27/28 Annual report *	Complete an annual report detailing key trends and findings for each of the technical remediation services via an agreed format.	31st March 2028

1. * Please note, this Milestone/Deliverable is outside of the current contract and is subject to a contract extension being approved

8. Management information/reporting

1. Management and reporting will be determined at each commissioned Work order.
2. Reporting will be in line with the requirements listed in the High-Level Capabilities document that can be found in the supplier document folder on Atamis. These requirements will form part of the contract.
3. The supplier will be required to create and maintain a supplier service delivery tracker, the main purpose of the tracker it to track

and manage all requests for technical remediation from initial onboarding through to completing delivery, this should include but not be limited to.

1. Recipient organisations request information and reference numbers
2. Supplier reference numbers.
3. Finances, covering work that is completed, and a forecast of future spend
4. Overview, maintain a report of the services that in the scope organisations have consumed
5. Issue log, used to capture issues and manage them through to resolution / closure.
6. Reporting, provide a weekly update to NHS England on progress, as per an agreed format.

4. The supplier will be required to maintain the existing trend analysis reporting, The purpose of this information is to capture data from the outcome of technical remediation services in a spreadsheet and then reporting back to NHS England on key trends and findings.
5. The supplier will be required to maintain the existing Heartbeat report, the purpose of this information to capture what services the organisations in scope have / haven't consumed.
6. The supplier will be required to complete the service delivery tracker created by Cyber Operations to support invoice approvals on a monthly basis. This will capture request reference numbers, ODS and organisation name and what month the work was completed amongst other things.
7. The supplier will create an annual report detailing key trends and findings for each of the technical remediation services via an agreed format.
8. The Supplier shall be responsible for ensuring any tools and equipment used to conduct technical remediation services within Health and Care Organisations is returned, NHS England will not accept the risk and costs of any items not returned.
9. The Supplier must not add unacceptable risk to an organisation as part of carrying out remediation services.
10. The supplier should evidence that all work achieves value for money and drives improvements via efficiency and effectiveness of the services over time

9. Volumes

1. The Order Contract is non-exclusive, and the Authority cannot guarantee volumes of work as part of this Contract.

2. Expected volumes will be determined by the allocated spending envelope each financial year
3. Each spending envelope allocation will be documented via an NHSE England Statement of work detailing the authorities' requirements that is agreed between both parties.
4. The Authority is working on the creation of a delivery pipeline (backlog) for the supplier to deliver financial year 25/26, ending 31st March 2026.
5. Technical remediation services are optional, and work is delivered as and when service recipients draw down the service.
6. NHS England in collaboration with Department of Health and Social Care's (DHSC) Joint Cyber unit (JCU) will provide the strategic direction confirming the organisations in scope and if any services are to be mandated.
7. In the absence of confirmed volumes, the following information is provided as indication to assist suppliers with your bids. The following table indicates the volumes / demand of the previous 12 months, including market share and proportion of available budget per item, volumes are expected to increase throughout the duration of the contract.

Service Types	Volume of Service types	% market share	% proportion of available budget
Bespoke technical remediation	41	31%	45%
Active directory review	29	22%	5%
MFA Policy Gap Analysis and Planning *	18	13%	8%
Secure backup reassessment	12	9%	1%
RBA Accelerator - Domain boundary *	11	8%	33%
Secure backup review	10	7%	3%
Vulnerability Management Maturity Assessment *	8	6%	2%
Network Segregation Review *	4	3%	1%

1. * RBA Accelerator - Domain boundary, RBA Accelerator - Server Zoning Extension, MFA Policy Gap Analysis and Planning, Vulnerability Management Maturity Assessment and Network Segregation Review demand forms part of an exercise completed in the last 12 months to enhance the TR service

catalogue. The figures represent the organisations that signed up to be early adopters as the products were developed and tested, demand is expected to increase as the products become more widely available.

8. Organisations currently in scope for technical remediation services
    1. NHS Trusts
    2. Integrated Care Board (ICB)
    3. Commissioning support unit (CSU)
    4. Arm's length bodies (ALB)
    5. 14x Select Community interest companies (CIC) who provide 2-hour urgent care response
9. The Authority will develop and implement a communications plan to increase awareness and utilisation of the technical remediation service catalogue. To include, but not limited to the following approaches
    1. General, this plan will include written communications and attendance at conferences, webinars etc to inform Health and Social Care organisations of the biggest threats and how technical remediation can help them identify issues/risks and support with the appropriate technical remediation activities.
    2. Targeted, predominantly via the Cyber regional security leads (RSL) and through use of a Heartbeat report and Trend analysis data the NHSE will target in scope organisations that have not consumed technical remediation services or have consumed discovery related technical remediation services to follow up and provide remediation support, initially focussing on the organisations that are considered the highest risk.
10. Provisionally a budget of [redacted] (including VAT) has been allocated for financial year 25/26, 1st April 2025 to 31st March 2026. Please note this information is indicative and subject to change.
11. A draft NHS England Statement of work has been included, Annex 9 - Cyber Technical remediation - Next Generation SoW 1 v1.0. Please note this information is indicative and subject to change, the statement of work will be finalised with the winning bidder to populate the spending envelope. This is to be confirmed and agreed with both parties following contract award.

10. Continuous improvement

1. The supplier should demonstrate how they can continually look to improve the service within the budget envelope. These may range from increasing the number of remediation services covered

with the data collected, better reporting or reducing the burden on the health and care organisation.
2. The Cyber Operations team carry out annual customer engagement using survey tools. If areas of improvements are identified this will be shared with the supplier to address.
3. The supplier should present improvements to the Authority's during regular service review meetings.
4. Changes to how the services are delivered must be brought to the Authority's attention and agreed upon before any changes are implemented.

11. Quality

1. The supplier's approach to the quality assurance process to ensure that the deliverables are of a high standard meet the relevant ISO 27001 standard and other quality standards detailed in the high-level requirements document.
2. All services and products provided under this contract must meet accessibility requirements, as described in the NHS digital service manual and GOV.UK. This applies to:
    1. **Digital services**: Websites (anything that runs in a browser and uses web technologies), mobile apps, intranets, third-party programs and tools, portals and any other online platforms.
    2. **Non-digital products**: Printed materials, physical forms, and other offline documentation.
    3. **Content and documentation**: Word documents, PowerPoint presentations, and any other downloadable or shareable content associated with the service

12. Price

1. Prices are to be submitted via the e-Sourcing Suite Atamis as an uploaded Price Schedule Template (in the Commercial Envelope) excluding VAT and including all other expenses relating to Contract delivery.
2. The Authority is unable to provide details on the size and scale of Health Care organisations at this current time, therefore we are requesting that the Supplier should use their knowledge and understanding in delivering such services, and applying the accurate resources for the types of works into a unit cost.
3. Work will be commissioned through work packages known as Statement of works (SoW); SoW are typically 1 of the following methods.
    1. **Standard**, defined as a work package that consists of set scope that is consumed on a 1 to many bases. E.g. Secure backup review

2. **Bespoke**, defined as a work package that is adhoc / bespoke based on the recipient organisations requirements that is consumed on a 1 to 1 basis. E.g. bespoke technical remediation

4. Each work package will be developed based on T&M, resulting in a fixed price. the work package will then be broken down into milestones.

13. Staff and customer service

1. The supplier shall ensure that staff understand the Authority's vision and objectives and provide excellent customer service to the Authority's throughout the duration of the Contract.
2. The supplier must have proven and demonstrable experience of delivering technical remediation services within government organisations and be able to supply references if required.
3. The supplier must have proven and demonstrable understanding of delivering DSPT within government organisations.
4. The Supplier must have proven and demonstrable understanding of the Cyber Assurance Framework (CAF).
5. The supplier must have proven and demonstrable experience of advising and reporting security focused remediation advice within government organisations.
6. The consultant should hold relevant compliance, technical or commercial roles.
7. The supplier must agree that all technical remediation work will be undertaken by experienced staff that hold National Security Vetting to a minimum of Security Check (SC) level.
8. The Supplier must have industry approved technologies and licensed or open-sourced tools to carry out either remote or onsite technical remediation activities. No data captured during the delivery should be removed in any form. This includes usernames, passwords extracted from tested servers and especially any sensitive data or personal data.
9. The Supplier will need to integrate their request process with the NHS England's standard ways of working, this means all new requests will need to be routed from the NHS England's Service desk to the supplier.

14. Security and confidentiality requirements

1. Supplier Staff shall be subject to pre-employment checks that include, as a minimum: verification of identity, employment history, unspent criminal convictions and right to work, as detailed in the HMG Baseline Personnel Security Standard (https://www.gov.uk/government/publications/government-

baseline-personnel-security-standard), as may be amended or replaced by the Government from time to time.

2. The Supplier shall agree that all Supplier Staff roles, i.e. project management, testing teams and any staff member managing a Work Order have specific government National Security Vetting clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

3. The Supplier shall provide and maintain a breakdown of the security clearance held for each Supplier Staff role and named individual and shall work with the Buyer to propose any necessary amendments to these in order to provide the Services.

4. The Supplier shall prevent Supplier Staff who have not yet received or are unable to obtain the security clearances required by this paragraph from accessing systems which store, process, or are used to manage Government Data, or from accessing Buyer Premises, except where agreed with the Buyer in writing.

5. 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, and the Supplier must be able to demonstrate the completion of the training for all in scope staff.

6. Where Supplier Staff are granted the ability to access Government Data or systems holding Government Data, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need such access but remain employed by the Supplier's organisation, their access rights shall be revoked by the close of business on the following Working Day.

7. When staff no longer need such access and they leave the Supplier's organisation, their access rights shall be revoked by the close of business on the same Working Day.

8. Specific security requirements, vetting and/or accreditation concerning the Supplier's staff and their systems are covered at the Requirements section of this ITT. Suppliers shall confirm their adherence to the requirements which is a pass/fail option. Suppliers not meeting these high-level requirements will not be evaluated any further in the process.

9. Confidentiality/security restrictions regarding the content of any requirements and/or the results/deliverables of the Requirement will be addressed at Work Order level.

15. Payment and invoicing

1. Payment - Is 30-day payment terms from invoice date. 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';
2. 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

3. The supplier will be required to complete the service delivery document created by Cyber Operations to support invoice approvals on a monthly basis. This will contain as a minimum the;
    1. ODS code.
    2. Site name.
    3. ServiceNow reference number.
    4. Type of work completed
    5. Month the work was completed.
    6. Discount applied at invoice level where/when applicable
4. All invoices will be issued as per the NHSE standard invoicing process and ensure that they have a clear level of detail, including a mandatory purchase order number, to support invoice approval and payments.
5. Invoices should be submitted once a payment milestone documented in the work order is completed and the necessary documentation (where applicable) to the NHS England portal. Invoicing will default to being issued at the end of the calendar month in which the work is delivered
6. All invoices will be issued as per the NHSE standard invoicing process detailed in 14.2 and ensure that they have a clear level of detail, including a mandatory purchase order number, to support invoice approval and payments.
7. The supplier will assume the risk for NHS Health and Care organisations cancelling or postponing an assessment before it starts, if cancelled then scheduling cost can only be invoiced.
8. Any additional costs associated with scope outside of what is originally agreed should be agreed with NHS England in advance of the work proceeding and documented and approved via Change control note (CCN)

16. Contract management

1. Attendance at service/contract review meetings shall be at the supplier's own expense. Although, where possible all meetings will be held via Microsoft Teams online meetings.
2. Upon Contract Award, each Supplier will be required to join a kick off call with the Authority's Cyber Operations Team.
3. If a Critical vulnerability is discovered, communication is expected as soon as details are fully confirmed. This can be via email and can be followed up via a call if required by the NHS Health and Care Organisation.
4. The Supplier shall provide a report review call, and ensure it is scheduled with 2 days of final report being delivered to relevant parties. The Supplier shall join a service review call with the CO to discuss service performance, reporting, invoicing, improvements, and progress of escalations as a minimum.
5. Technical remediation services will typically be performed remotely, There may be some instances where an on-site review is requested, where this is the case, the supplier, NHS England and the Health and Care Organisations should adhere to current government guidelines

17. Social value

1. Social value forms part of the technical response envelope of the tender submission.
2. Social value responses and commitments will form part of the Order form.

18. Location

1. Technical remediation services will typically be performed remotely, there may be some instances where an on-site review is requested, where this is the case, the supplier, NHS England and the Health and Care Organisations should adhere to current government guidelines

19. Appendix

1. **Appendix 1 – Work Order Process (request fulfilment)** - This Work Order should be read in conjunction with the terms of the Call-Off Contract between the parties dated [insert date when known] and the terms of the Call-Off Contract form part of this Work Order including but not limited to any limitations of liability therein.
    1. Technical remediation requests are received as and when internal team's (Health and Care Organisations) requirement arises. Requests come into NHS England via our in-house system ServiceNow.

2. The request is reviewed initially by the Cyber Operations team and once it is deemed sufficient in detail to share and within scope, the Cyber Operations will issue the new request to the supplier that is appointed the contract using ServiceNow.
3. The supplier will manage all aspects of the customer onboarding from this point through to completion of the delivery. This will consist of
4. Reaching out to the customer within two business days to arrange an onboarding call. This call will set out the expectations with the recipient organisation including resource commitment, data needed to run the tests, and devices they may need to setup to run cyber tests.
5. The supplier needs to keep the recipient organisation informed of progress, and highlight any critical issues found immediately
6. Hold a close out call / debrief with the recipient organisation to discuss findings and recommendations how to correct issues found.
7. The supplier will provide the outputs of each work order will be provided to recipient organisation and stored on NHSE SharePoint location. If any output contains personal data, this must be removed before they are provided to NHS England. If the report contains sensitive data (e.g., IP address details) this should be redacted in the version of the report being sent to NHS England.
8. The supplier will complete reporting as per an agreed format
9. The supplier should notify the Cyber Operations team that the work is completed so the request can be closed within the ServiceNow toolset

2. **Appendix 2 - High level bespoke technical remediation scoping process**

#	Task	Summary	Estimated Lead time
1	New request raised via ServiceNow – triage and validation	Live services Cyber (LSC) to complete triage and validation of the request seeking endorsement that the request • Cannot be fulfilled by other	1-5 days

		means e.g. another national service. • The requesting organisations has not already received funding for this requirement. The outcome will be increased cyber capabilities and resilience to reduce the risk of a Cyber-attack.	
2	Supplier Feasibility check	Supplier will be responsible for receiving the service request from NHSE and initially conducting feasibility checks to review the recipient organisations requirements and confirm • Supplier has the capabilities to scope and deliver bespoke remediation, • Supplier has capacity to deliver desired scope within the contractual constraints Provide a high-level summary how you propose to meet this demand including a rough order of magnitude (ROM).	2-3 days
3	Regional security lead agreement in principle (by exception only)	Managed by exception, regional security lead agreement in principle to be obtained • If supplier only has partial capability • and/or partial capacity	1-5 days

		and/or the ROM cost exceeds 50k	
4	Suppliers scope the requirements	Supplier will coordinate the recipient organisation to scope the requirements and document via a Statement of work. SoW should include all aspects listed within Appendix 3 – Statement of works requirement	5-10 days (following scoping call)
5	Requestor review	Supplier will coordinate the recipient organisation to review a Non-Commercial SoW to review and confirm scope meets their requirement, and ensure the pre-requisites are understood and the correct personnel, materials and other preparatory activities are conducted.	5-10 days
6	NHSE review	Supplier will coordinate NHSE nominated stakeholders to review the Commercial SoW to ensure the service is appropriately scoped, features the correct activities and isn't overboard on the required resources/time, and confirm approval	1-5 days
7	Scoping complete	Supplier will undertake documented activities against an agreed statement of work.	Adhoc

3. **Appendix 3 – Statement of works requirement** - The statement of work (SOW) is a legally binding document that captures and de-fines all the work management aspects of your project. You will note the activities, deliverables, and timetable for the project. There are two types of Statement of works.

1. Standard SoW – shared with recipient organisation and excludes any commercial sensitive information and only covers the scope.
2. Commercial SoW – shared with NHS England only, this document includes the above with the additional of commercial information.

Supplier statement of work must include the following as a minimum.

3. Background Information – a brief introduction for your project, why is the request required / problem statement.
    1. Define the purpose of your project.
    2. Why are you initiating this project?
    3. What's the purpose of the project?
    4. How will it address the problem statement?
    5. What are the project objectives, deliverables and return on investment?
    6. How will this reduce risk?
4. Scope of the requirements -Detailed overview of the scope, a breakdown how the service offering phases will be delivered, what tasks / deliver-able are to be completed, including outputs / acceptance criteria for each phase.
5. Out of scope items
6. Prerequisites for the supplier to deliver the services - general and /or phases.
7. Roles and responsibilities – Covering supplier, recipient organisation, authority and any mutual
8. Project schedule / delivery plan
9. Risk, Assumptions, Issus and dependencies (RAID)
10. Finances / payment milestones.
11. Approvals

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)
- doesn't 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 doesn't 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, 12.2 or 14.8 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 The Supplier indemnifies CCS and every Buyer against any costs resulting from any Default by the Supplier relating to any applicable Law to do with a Contract.

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 14.7 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 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.