# DPS Schedule 6 (Order Form Template and Order Schedules)

# Order Form

| | |
|---|---|
| ORDER REFERENCE: | C169824 |
| THE BUYER: | UK Health Security Agency |
| BUYER ADDRESS | Nobel House, 17 Smith Square, London, SW1P 3HX |
| THE SUPPLIER: | NCC Group Security Services Limited |
| SUPPLIER ADDRESS: | Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ |
| REGISTRATION NUMBER: | 04474600 |
| DUNS NUMBER: | 64-071-1540 |
| DPS SUPPLIER REGISTRATION SERVICE ID: | |

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 15/05/2023. It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
Not applicable

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 and the Statement Of Works contained in Order Schedule 4 (Order Tender).
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) – Not applicable
  - Joint Schedule 10 (Rectification Plan)
  - Joint Schedule 11 (Processing Data)

---

- Order Schedules for RM3764iii
  - Order Schedule 1 (Transparency Reports)
  - Order Schedule 2 (Staff Transfer)
  - Order Schedule 5 (Pricing Details)
  - Order Schedule 6 (ICT Services) - Not applicable
  - Order Schedule 7 (Key Supplier Staff )
  - Order Schedule 8 (Business Continuity and Disaster Recovery)
  - Order Schedule 9 (Security)
  - Order Schedule 10 (Exit Management)
  - Order Schedule 13 (Implementation Plan and Testing)
  - Order Schedule 14 (Service Levels)
  - Order Schedule 15 (Order Contract Management)
  - Order Schedule 18 (Background Checks)
  - 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

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 Parties agree that:

(1) Annex A (Order Special Terms Annex) shall apply to this Order Contract;

(2) clause 14.3 of the CCS Core Terms (DPS version) shall not apply to this Order Contract.

(3) clause 3.1.2 of the CCS Core Terms (DPS version) shall not apply to this Order Contract.

(4) subject to the remainder of this clause, the Supplier may elect to notify relevant third party software and systems vendors of the existence of critical vulnerabilities discovered during performance of the Services. The Supplier

will only make such a notification where it reasonably considers that the existence of the vulnerability should be brought to the relevant vendor's attention to prevent harm to other users of the software or systems, and that the Supplier making the notification is generally in the public interest. The Supplier will limit the content of any notification to the existence of the vulnerability in question, and will not provide any data or information specific to the Buyer or which might reasonably be expected to identify the Buyer. In all cases, the Supplier will never make such a notification in a way that would cause the Supplier to breach its obligations owed to the Buyer regarding confidentiality and data protection, or any other provision of the Order Contract unless it is required to do so by law;

(5) the Services cannot be cancelled. Subject to clause 5.3 below, any Charges paid or payable in relation to Services are non-refundable.

(6) In the event of termination of the Order Contract, subject to clause 7 below:
6.1. the Supplier will be entitled to retain all Charges paid (and to be paid immediately for all amounts that are as at that date invoiced but unpaid) and no refunds or credits will be given; and
6.2 the Buyer will immediately pay any unpaid Charges that would have been payable in respect of the remainder of the term of the Order Contract following the effective date of termination but for such termination.

(7) Notwithstanding clause 5, where the Order Contract is terminated due to material breach by the Supplier, the Supplier shall refund any pre-paid Charges covering the remainder of the term of the Order Contract after the effective date of termination and the Buyer shall not be required to pay any Charges that would have been payable in respect of the remainder of the term of the Order Contract following the effective date of termination but for such termination.

(8) Notwithstanding any other provision of clauses 5, 6 and 7, in no event will termination, irrespective of the reason or circumstance, relieve the Buyer from paying: (i) Charges in respect of the period prior to the effective date of termination; and (ii) any Set Up Charges (as defined in Annex A) that would have been payable in respect of the remainder of the term of the Order Contract following the effective date of termination but for such termination, which shall become payable immediately on termination.

(9) Services cannot be postponed by the Buyer beyond the start date of the Services save by mutual agreement between the parties, and subject to the payment of any additional Charges payable thereunder. and

(vi) these Order Special Terms do not amount to a material change of the CCS Core Terms (DPS version) and/or the Order Contract and are within the meaning of the Regulations and the Law.

ORDER START DATE: 19/05/2023

ORDER EXPIRY DATE: 18/05/2024

ORDER INITIAL PERIOD: 12 Months

ORDER OPTIONAL EXTENSION 2 x 12 months extension options. The Buyer shall provide no less than 3 months' written notice to the Supplier of its intention to extend the Order Contract.

DELIVERABLES
Deliverables as defined below;

1. Key milestones and deliverables
   1.1. The Cyber CSOC provision within the Buyer is currently provided by a combination of service providers and contract staff under the PSR framework. These contracts come to an end in March 2023.
   1.2. Following on from the Start date the Supplier will
      1.2.1. Propose a service improvement plan within 12 weeks. The plan should detail the opportunities for increasing the level of service provided by the CSOC as well as providing opportunities for efficiency saving and service improvements.
      1.2.2. During the term of the Order Contract the Supplier will implement the agreed first stage improvements and be in a position to manage a continuous improvement cycle as further described in this Order Contract.
   1.3. Suppliers should note that, where the Buyer requests in writing that staff are required to hold Security Check (SC") security clearance, it should be able to provide staff with current SC clearances
   1.4. The following Contract milestones/deliverables shall apply:

| Milestone/Deliverable | Description | Timeframe or Delivery Date |
|---|---|---|
| Kick off/Initiation Meeting | Contract commences with an opportunity to reconfirm scope and deliverables subject to (i) the variation procedure set out in the Core Terms (DPS version) and (ii) clause 5 of the Order Special Terms. To gain additional information and context regarding the Buyers organisation and to further clarify the scope | Within week 1 of Contract Award |

| | | |
|---|---|---|
| Onboarding | Onboarding of Services | Within week 4 of Contract Award or no later than 19/05/2023 |
| Progress Meeting/Technical Testing | Produce a report outlining all findings, remediation steps for each, and an evaluation of the Buyers vulnerability management system. | progress meeting during discovery weekly and then one final presentation at the end. Once into implementation the progress meetings would be monthly with a Kick off and then a wrap up. During service delivery there will be a monthly account meeting. |
| Ongoing SOC Operations | Daily operations of the SOC such as triaging and investigating alerts report. | Ongoing of the final deliverable |
| Monthly Reporting | Reports are created and delivered monthly to inform the Buyer of the threats remediated, whilst providing insight into the security operations affecting the Buyer. | Monthly reports |

The detailed description of the Services and Deliverables is contained in Order Schedule 4 (Order Tender) and, in regards to MDR Services, sections 1, 2, 4, 5.1, 5.3 and 7 of the Supplier's MDR Master Service Description and SLA Document attached hereto as a separate document.

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 £2,622,740

ORDER CHARGES
The rate card is as detailed in Supplier's pricing bid embedded below;

Pricing-Schedule-NC C%20Group%200603

The parties agree that the value of the Order Contract for Year 1 is £2,622,740 excluding VAT and expenses of which £1,124,870 excluding VAT and expenses (value of MDR Services) is a fixed value. Detailed breakdown of Charges and invoicing profile are contained in Order Schedule 5 (Pricing Details).

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD
BACS

BUYER'S INVOICE ADDRESS:

Accounts Payable, UK Health Security Agency, Manor Farm Road, Porton Down, Salisbury, SP4 0JG, UKHSA VAT No: GB888851648

payables@phe.gov.uk

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]
BUYER'S ENVIRONMENTAL POLICY
N/A

BUYER'S SECURITY POLICY
N/A

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]
SUPPLIER'S CONTRACT MANAGER
[redacted]
PROGRESS REPORT FREQUENCY (only applicable to MDR Services)
Each calendar month

PROGRESS MEETING FREQUENCY (only applicable to Security Improvement Services)
As per the “”Progress Meeting/ Technical Testing” section contained within a table in the “Deliverables” section above

KEY STAFF
As listed in Annex 1 to Order Schedule 7 (Key Supplier Staff)

KEY SUBCONTRACTOR(S)
Not applicable

COMMERCIALLY SENSITIVE INFORMATION
N/A

SERVICE CREDITS
In relation to the MDR Services, Service Credits and Service Levels are as detailed in the Order Schedule 14 (Service Levels).

Service Credits and Service Levels are not applicable to the Security Improvement Services.

ADDITIONAL INSURANCES
N/A

GUARANTEE
N/A

SOCIAL VALUE COMMITMENT
N/A

**For and on behalf of the Supplier:**

[redacted]

**For and on behalf of the Buyer:**

# Annex A

## Order Special Terms Annex

1 Additional Terms

1.1 The Buyer and the Supplier agree that the terms contained within this Order Special Terms Annex **("Annex")** shall form part of the Order Contract. To the extent that there is any conflict between (i) this Annex and (ii) the CCS Core Terms (DPS version), the terms contained within this Annex shall take precedence.

1.2 Annex 1 of this Annex A apply to MDR Services. The Schedules attached to the Annex 1 set out additional terms and conditions that are applicable to the MDR Service Offerings.

1.3 To the extent that there is any conflict between (i) Clauses 1-10 of the Annex 1 and (ii) a Schedule to the Annex 1, the relevant Schedule shall take precedence in respect of the applicable MDR Service Offering to which it relates.

1.4 Annex 2 of this Annex A apply to Remediation Services.

## Annex 1 (Managed Detection and Response Services)

1. Definitions:

"**Alert**" means a response to the correlation of one or more individual Events processed by an MDR Service Offering, generated by such MDR Service Offering where a potential situation requires analysis and investigation;

"**Annual Charges**" means those Charges payable by the Buyer each Order Contract Year for the ongoing provision of the MDR Services, as set out in the SOW (and excluding, for the avoidance of doubt, the Set Up Charges);

"**CIRT**" means the Supplier's cyber incident response team;

"**Order Contract Year**" means each successive period of 12 months from the Relevant Go Live Milestone during which the MDR Services are to be provided;

**"Equipment"** means hardware or software provided by the Supplier to the Buyer to assist in delivery or performance of Services;

"**Event**" means an individual item of machine data which is generated as a response to an action, change or series of actions and changes made to an IT system or network providing visibility as to the timing and nature of the action or change;

"**End User Licence Agreement**" means the end user licence agreement or similar document that the Buyer is required to enter into directly with the relevant third party vendor to enable the Buyer to use and receive the Third Party Software;

"**False Positive**" means an alarm which is generated indicating that a security incident has occurred which subsequent investigation determines is incorrect;

"**Go Live Milestone**" means in respect of a particular MDR Service Offering, the earlier of (i) 12 weeks from the date of acceptance of the applicable Statement of

Work and (ii) the date The Supplier confirms in writing to the Buyer that the Set up Services have been completed;

"**Managed Detection & Response Services**" or "**MDR Services**" means the portfolio of managed detection and response services to be delivered by The Supplier from the SOC and/or CIRT, as described in the relevant Service Description and which are the subject of the Order Contract;

"**MDR Portal**" means the The Supplier Assist Live portal (or any alterative portal) made available for access by the Buyer as part of the MDR Services, for the purposes of providing secure communications, information exchange, incident management (ticket and incident data), and real time performance metrics;

"**MDR Service Offering**" means an individual service offering which forms part of the MDR Services;

"**MSP Software**" means any software (including any derivatives of such software) owned by a third party and licensed to the Supplier that the Supplier agrees to make available for use by the Buyer on an MSP basis as an integral part of the Services, as specified in the Order Contract or the Statement of Works;

"**Normal Office Hours**" means 8am – 6pm (GMT) on any day which is a Working Day;

"**Onboarding Form**" means the applicable onboarding form requesting pre-Service information from the Buyer, to be completed by the Buyer and returned to the Supplier within 5 Working Days of receipt from the Supplier;

"**Relevant Go Live Milestone**" means the date which is the earliest of the respective Go Live Milestones for all MDR Services to be provided under the Order Contract;

"**Relevant Systems**" means any systems, networks, hardware or software which the Buyer requires to be monitored or investigated (as applicable) as part of the MDR Services, together with any software, systems, networks, premises, equipment, data structures, protocols, computers, hardware and firmware linked to the same and data passing across or contained in any of the foregoing;

**"Service Level(s)**" means the applicable service level(s) that shall apply to the MDR Service Offerings, as contained in the Order Schedule 14 – Service Levels;

"**Service Level Appendix**" means the relevant section or appendix to the Service Description setting out the Service Levels (if applicable) to the MDR Service Offerings;

"**Service Level Start Date**" means, in respect of each Service Level, the date which is 4 weeks from the applicable Go Live Milestone or such other date as is specified in the Order Contract and/or the applicable SOW;

"**Set Up Charges**" means (i) those Charges payable by the Buyer in respect of the Set up Services, and (ii) all licence Charges in respect of the Third Party Software and/or MSP Software, as specified in the Order Contract or the SOW;

"**Set up Services**" means the initial set up and installation services to be provided by the Supplier in respect of each MDR Service Offering, as set out in the Service Description and/or Statement of Work;

"**Service Description**" means the service description applicable to the MDR Services, as updated by the Supplier from time to time;

"**Site(s)**" means the location(s) which the Buyer has advised the Supplier in the Onboarding Form that the Supplier Equipment will be located or, where no such site is stated in the Onboarding Form, such location(s) as agreed between the parties;

"**SOC**" means the Supplier's 24 hour security operations centre;

"**Third Party Software**" means any software (including any derivatives of such software) owned by a third party that the Supplier agrees to supply to the Buyer on a resale basis as specified in the SOW or the Order Contract;

"**Third Party Vendor Terms**" means the specific terms and conditions that will apply to the provision and use of MSP Software, the current version of which is either included within the relevant Schedule to this Annex or is otherwise made available by the Supplier;

"**Working Day**" means any day other than a Saturday, a Sunday or any day which is a bank holiday in England and Wales;

"**Working Hours**" means a period of 8 hours during Normal Office Hours.

2 Buyer's Duties

2.1 The Buyer agrees:

2.1.1 to complete and return to the Supplier the relevant Onboarding Form by the Buyer within 5 Working Days of receipt from the Supplier;

2.1.2 to provide the Supplier with all information, assistance, approvals and authorisations as may be reasonably necessary to allow the Supplier to interface with the Relevant Systems and in order for the Supplier to provide the MDR Services;

2.1.3 without prejudice to clause 2.1.2:

2.1.3.1 to obtain, prior to the Start Date, all consents required from its ISP and any third party suppliers of the Relevant Systems together with such other consents required for the MDR Services to be carried out and provide written evidence of such consents upon NCC request;

2.1.3.2 if relevant, and prior to the start date of the Services, to notify relevant employees that the MDR Services are to be carried out and that they may be monitored;

2.1.3.3 to provide remote access to all Relevant Systems as necessary for the provision of the MDR Services;

2.1.3.4 to ensure that its Relevant Systems shall use Western character sets (and that the Supplier shall not be required to carry out the MDR Services on Relevant Systems which use non-Western character sets for the duration of the MDR Services,

2.1.3.5 to provide the Supplier with prompt access to at least one employee who shall have substantial computer systems, network and project management experience of the Systems and any other applicable systems, who shall act as liaison between the Buyer and the Supplier;

2.1.3.6 to inform the Supplier of any network or infrastructure changes that may impact the MDR Services or the Supplier's ability to provide the MDR Services;

2.1.3.7 to provide feedback to the Supplier from investigations carried out when an incident reported via the MDR Services is found to be a False Positive; and

2.1.3.8 at all times to co-operate with the Supplier and to provide the Supplier promptly with such other relevant information and appropriate log files about the Relevant Systems, network, premises, equipment, data structures, protocols, software, hardware and firmware as is reasonably required by the Supplier;

2.1.4 to comply with its obligations in respect of any NCC Equipment as set out in the applicable Schedule to this Annex or otherwise in this Order Contract or the statement of works;

2.1.5 where the MDR Services are to take place on the Buyer's premises:

2.1.5.1 to ensure that a suitable working space is provided for the Supplier's Personnel which shall include (without limitation) a desk and network access where appropriate; and

2.1.5.2 to indemnify, keep indemnified and hold harmless the Supplier and its Affiliates in full and on demand from and against all liabilities, direct, indirect and consequential losses, damages, claims, proceedings and legal costs (on an indemnity basis), judgments and costs (including without limitation costs of enforcement) and expenses which the Supplier incurs or suffers directly or indirectly in any way whatsoever arising out of or in connection with any claim or action against the Supplier for death and/or personal injury arising out of the Buyer's failure to provide safe premises;

2.1.6 to only use the MDR Services in support of the Buyer's own business operations;

2.1.7 to comply with any additional acceptable use policy or other terms of use which may be set out in the Service Description or which may otherwise be provided by the Supplier to the Buyer. In the event of any conflict between such policy or terms and the remainder of the Order Contract, the remainder of the Order Contract shall take precedence;

2.1.8 that the Supplier may retain information or data resulting from the MDR Services to the extent that it reasonably requires it to improve its managed detection and response services generally;

2.2 The Buyer shall assume all liability and shall indemnify, keep indemnified and hold harmless the Supplier and its Affiliates and its and their officers, employees, agents, contractors and sub-contractors in full and on demand from and against any and all third party claims (including, but not limited to, claims for alleged or actual infringement of Intellectual Property Rights), losses, damages, demands, costs, expenses, Charges (including, but not limited to, court and legal Charges) and liabilities (in each case whether direct, indirect or consequential) of whatever nature suffered, incurred or sustained by the Supplier directly or indirectly as a result of the failure by the Buyer to comply with its obligations under this clause 2.

3 Supplier's Duties

3.1 The Supplier shall notify the Buyer if any threat or malicious activity is detected through the MDR Services in accordance with the reporting mechanisms and principles agreed with the Buyer in the Onboarding Form and in line with the Service Description for MDR Services.

3.2 The Supplier shall, subject to the remainder of this Annex and with effect from the applicable Go Live Milestone for the relevant MDR Service Offering, provide the MDR Services in accordance with the applicable Service Levels provided that any remedies for failure to meet the Service Levels as set out in clause 3.3 below shall only apply from the applicable Service Level Start Date.

3.3 If the Supplier's provision of the MDR Services does not meet the applicable Service Levels in accordance with clause 3.2 above, the Charges for the MDR Services shall be adjusted in accordance with the Service Level Appendix, to the extent applicable. Such adjustment (and/or any other remedies specified in the Service Level Appendix) shall be the Buyer's sole and exclusive remedy for such failure to meet the Service Levels.

3.4 Any failure by the Supplier to achieve a Service Level or other obligation under the Order Contract shall be disregarded (and the Supplier shall not be considered in breach of its obligations hereunder) where such failure is caused by or related to:

3.4.1 a failure by the Buyer to comply with its obligations under the Order Contract; and/or

3.4.2 any event or circumstance which is beyond the reasonable control of the Supplier, including but not limited to:

3.4.2.1 any failure, disruption and/or error in the Relevant Systems;

3.4.2.2 ISP or third party software supplier (including AWS) failures or disruptions;

3.4.2.3 any failure, disruption and/or error in the Buyer's infrastructure upon which Supplier Equipment, Third Party Software or MSP Software is hosted;

3.4.2.4 an error or fault with the Supplier Equipment caused by a breach by the Buyer of its obligations in respect of such Supplier Equipment;

3.4.2.5 an error or fault with any Third Party Software, other than where caused by configuration by the Supplier of such Third Party Software as part of the MDR Services

3.4.2.6 any other event or circumstance specifically referred to in the applicable Schedule to this Annex 1, the Service Description and/or Order Form).

3.5 The Supplier will not be required to travel to such countries listed as "Advise against all travel" or "Advise against all but essential travel" by the Foreign Commonwealth Office (FCO) in its travel advice or to those countries where travel is restricted in accordance with the Supplier's internal policies.

4 Charges and Payment

4.1 Annual Charges for the MDR Services are payable annually in advance. The Supplier will invoice the Buyer for the first such payment upon the Relevant Go Live Milestone, and subsequent invoices will be raised upon each anniversary thereof during the term of the Order Contract. The Supplier will invoice the Buyer for the Set up Charges upon the acceptance of the Order Contract.

4.2 The Supplier shall be entitled to revise the Charges for the MDR Services at the end of each Order Contract Year by giving the Buyer written notice of such change not less than thirty (30) days' prior to the end of that Order Contract Year.

4.3 The Supplier shall be permitted to charge the Buyer additional Charges should additional services not specified within the Statement of Works become necessary or are requested by the Buyer.

4.4 All payments due under this Order Contract shall be made without any deduction by way of set off, counterclaim, discount or abatement or otherwise except where the Buyer is expressly permitted to do so by Order of Court.

4.5 Expenses for travel to a Buyer's location where required for the purposes of the MDR Services or any additional services agreed pursuant to clause 4.3 shall be chargeable in addition to the Charges.

5. MDR Portal

5.1 The Supplier grant to the Buyer during the Term a non-exclusive, royalty free, licence to access and use the MDR Portal solely to the extent necessary to receive the MDR Services and in compliance with the Supplier's acceptable use policy for such portal in force from time to time.

5.2 Ownership of all Intellectual Property Rights in the MDR Portal remains with the Supplier and nothingin the Order Contract will operate to transfer to the Buyer or to grant to the Buyer any other licence or right to use the MDR Portal.

5.3 The Supplier may at its absolute discretion suspend the Buyer's access to the MDR Portal at any time if the Buyer uses the MDR Portal in breach of the Order Contract or the applicable acceptable use policy.

5.4 The Buyer shall ensure that its access credentials for the MDR Portal are stored securely and only used by authorised employees and are not shared with any other person. The Buyer shall take all reasonable steps to prevent any unauthorised access to the MDR Portal and will immediately notify the Supplier if it becomes aware of any such access;

6. Liability

6.1 Subject to clause 11.4 of the Core Terms (DPS), the Supplier shall not be liable for any:

6.1.1 loss of or damage to the Buyer's, its agents' and/or its sub-contractors' property caused directly or indirectly by the Supplier's Equipment; or

6.1.2 disruption to the Relevant Systems or any loss of or corruption to any data and/or software during the period of the MDR Services; or

6.1.3 use or misuse of information accessed due to another party being informed of or gaining access to the Buyer's user names and passwords in connection with the MDR Portal.

6.2 The Buyer accepts and acknowledges that the MDR Services reflect the level of information reasonably available to the Supplier when performing such Services. As such, subject to clause 11.4 of the Core Terms (DPS), the Supplier does not warrant or guarantee the accuracy of the MDR Services beyond the date that they were performed, nor does the Supplier warrant or guarantee that any findings and conclusions contained in the Deliverables are exhaustive.

6.3 Supplier's Personnel will not be legally qualified. As such, subject to clause 11.4 of the Core Terms (DPS), the Buyer accepts and acknowledges that, while the Supplier and its Personnel may give opinions and recommendations based on its industry experience and expertise, the MDR Services and any associated Deliverables do not constitute legal advice, and the Buyer is advised to seek such independent legal advice if it feels it necessary to do so.

Schedule A SIEM Threat Detection Services

1 Interpretation

1.1 This Schedule B sets out the additional terms and conditions applicable to SIEM Threat Detection Services, and is to be read in conjunction with the remainder of this Annex.

2 Definitions:

"**SIEM Threat Detection Services**" means the security incident and event management services delivered by the Supplier from the SOC as described in the relevant Service Description and Order Contract or the Statement of Work;

"**SIEM Software**" means the security incident and event management software to be used for the purposes of the SIEM Threat Detection Services; and

"**MDE Software**" means the Supplier's managed detection application known as "Managed Detection Engine" or "MDE" or other similar proprietary software as the Supplier may provide as part of the SIEM Threat Detection Services, as specified in a Statement of Work or the Order Contract.

3 Managed SIEM – using Buyer directly acquired SIEM Software ('Bring Your Own SIEM')

3.1 The Buyer shall correctly install and configure the SIEM Software to enable the Supplier to provide the SIEM Threat Detection Services. To the extent agreed in an Order Contract or a SOW, the Supplier shall provide reasonable remote assistance in respect of such installation and configuration.

3.2 On an ongoing basis for the duration of the Order Contract, the Buyer shall provide the Supplier with all relevant: (i) details of; and (ii) access credentials and user rights in connection with, the SIEM Software as requested by the Supplier to enable it to perform the SIEM Threat Detection Services.

3.3 The Buyer shall procure and maintain appropriate licences to the SIEM Software specified in the Order Contract or the SOW for the term of the Order Contract to enable the Supplier to perform the SIEM Threat Detection Services. For the avoidance of doubt, where the Buyer has procured, or will procure, the SIEM Software directly (and not from or via the Supplier), such SIEM Software is not Third Party Software or MSP Software for the purposes of the Order Contract and the Supplier has no responsibility for the performance or operation of the same and shall not be liable for any breach of the Order Contract to the extent that it was caused (directly or indirectly) by the Buyer's failure to comply with this clause 3.

3.4 The Buyer confirms that it has obtained all necessary consents in respect of the SIEM Software to enable the Supplier to carry out the SIEM Threat Detection Services

including but not limited to the consent of any relevant third party service providers and/or third party software vendors.

4 MDE Software

4.1 Where a Statement of Work or the Order Contract specifies that MDE Software is to be provided, the Supplier grants to the Buyer a non-exclusive, non-transferable licence for the term of the Order Contract to use the MDE Software, solely in relation to the MDR Services.

4.2 Ownership of all Intellectual Property Rights in the MDE Software remains with the Supplier and nothing in the Order Contract will operate to transfer to the Buyer or to grant to the Buyer any other licence or right to use the MDE Software.

4.3 The Supplier may at its absolute discretion suspend the Buyer's access to the MDE Software at any time if the Buyer uses the MDE Software in breach of the Order Contract or the applicable acceptable use policy.

4.4 Upon expiry of termination of the Order Contract, the Buyer shall cease all use of the MDE Software, and shall confirm in writing to the Supplier that it has done so.

# SCHEDULE B MANAGED ENDPOINT DETECTION & RESPONSE

## 1 Contract Structure and Interpretation

1.1 This Schedule B sets out the additional terms and conditions applicable to Managed Endpoint Detection & Response Services and is to be read in conjunction with the remainder of this Service-Specific Module.

## 2 Definitions:

“Endpoint Software” means third party end point detection technology, which comprises Endpoint Agents and the Endpoint Detection Platform;

“Endpoints” means the computer devices on which the Endpoint Agents are installed, including but not limited to, laptops, desktops, tablets and servers;

“Endpoint Agents” mean third party sensor software used to collect telemetry data from the Endpoints and to communicate such data to the Endpoint Detection Platform;

“Endpoint Detection Platform” means a third party cloud based management platform used to collect telemetry data from the Endpoints in one central repository;

“Managed Endpoint Detection & Response Services” means the process of assessing the Endpoints for malicious traffic using (i) Endpoint Software , (ii) proprietary threat intelligence and (iii) remote analyst reviews, triage & investigation of threats; and

“Site(s)” means the location(s) which the Buyer has advised Supplier in the Onboarding Form that the Endpoint Agents will be installed or, where no such site is stated in the Onboarding Form, such location(s) as agreed between the parties.

## 3 Buyer’s Duties

3.1 The Buyer shall correctly install and configure the Endpoint Agents to the Relevant Systems at the Site(s) and where in scope in accordance with Supplier’s instructions. Supplier shall provide reasonable remote assistance in respect of such installation and configuration to the extent detailed in the Statement of Work.

3.2 Upon expiry or termination of the Contract, the Buyer shall immediately cease use of the Endpoint Agents and shall confirm in writing to Supplier that it has done so.

3.3 On an ongoing basis for the duration of the Contract, the Buyer shall provide Supplier with all relevant: (i) details of; and (ii) access credentials and user rights in connection with, the Endpoint Software, as requested by Supplier to enable it to perform the Managed Endpoint Detection & Response Services.

3.4 The Buyer shall procure and maintain appropriate licences to the Endpoint Software specified in the Statement of Works for the term of the Contract to enable Supplier to perform the Managed Endpoint Detection & Response Services. For the avoidance of doubt, where the Buyer has procured, or will procure, the Endpoint Software directly (and not from or via Supplier), Supplier has no responsibility for the

performance or operation of the same and shall not be liable for any breach of the Contract to the extent that it was caused (directly or indirectly) by the Buyer's failure to comply with this clause 3.

3.5 The Buyer confirms that it has obtained all necessary consents in respect of the Endpoint Software to enable Supplier to carry out the Managed Endpoint Detection & Response Services including but not limited to the consent of any relevant third party service providers and/or third party software vendors.

Schedule C – Retained Incident Response (RIR)

1 Order Contract Structure and Interpretation

1.1 This Schedule C sets out the additional terms and conditions applicable to Retained Incident Response Services where provided as Managed Detection Response Services, is to be read in conjunction with the remainder of this Annex.

2 Definitions:

"**Alert Analysis and Investigation**" means the initial remote support services provided by SOC to the Buyer to advise on the containment and/or remediation of an Alert (prior to the activation of Retained Incident Response Services);

"**Alert Investigation Period**" means the maximum period of time SOC will spend undertaking Alert Analysis and Investigation, as set out in the Service Description.

"**CIRT**" means he Supplier's Cyber Incident Response Team;

"**CIRT Triage Investigation Approval**" has the meaning ascribed to it in clause 3.2;

"**CIRT Triage Investigation Period**" means the maximum period of time CIRT will spend undertaking CIRT Triage Investigation prior to the issuance of a RIR Response Proposal, as set out in the Service Description;

"**CIRT Triage Investigation**" means the initial investigation of an Alert by CIRT following completion of Alert Analysis and Investigation;

"**Normal Office Hours**" means 8am – 6pm

**"Retained Incident Response Services" or "RIR Services**" means the incident response services provided by the CIRT as described in the Service Description and the Statement of Works, including CIRT Triage Investigation;

"**Report**" means any report produced by the Supplier detailing the results of the Incident Response Services;

"**RIR Proposal Approval**" has the meaning ascribed to in clause 3.3.

"**RIR Response Proposal**" has the meaning ascribed to it in clause 3.3;

"**RIR Service Request**" has the meaning ascribed to it in clause 3.3;

3 Activation of Retained Incident Response Services

3.1 In the event an Alert cannot be contained or remediated by SOC within the Alert Investigation Period, or where this cannot be executed remotely by SOC as part of Alert Analysis and Investigation, SOC may recommend to the Buyer that an Alert be passed to CIRT for CIRT Triage Investigation.

3.2 Upon receipt of written approval from the Buyer for the Alert to be passed to CIRT for CIRT Triage Investigation ("**CIRT Triage Investigation Approval**"), CIRT will commence the provision of CIRT Triage Investigation. Time spent undertaking CIRT

Triage Investigation is chargeable by the Supplier, for which the Minimum Call Off Days will be used (where available).

3.3 Upon expiry of the CIRT Triage Investigation Period, CIRT will inform the Buyer and the Buyer may make request for further Retained Incident Response Services in respect of the relevant Alert ("RIR **Service Request**"). Once a RIR Service Request has been logged the Supplier shall prepare in writing a proposal setting out the scope of the work to be carried out by the Supplier in relation to the relevant RIR Service Request (a "**RIR Response Proposal**").

3.4 Upon receipt of written acceptance from the Buyer of the RIR Response Proposal ("**RIR Proposal Approval**"), The Supplier shall provide the Retained Incident Response Services set forth in the RIR Response Proposal (including any Additional Services) to the Buyer.

4 The Supplier Duties

4.1The Supplier shall carry out the Retained Incident Response Services in accordance with the terms and conditions set forth in the Order Contract, using reasonable care and skill and in a professional manner.

4.2 Where a Report is required it shall, unless otherwise stated in the Response Proposal or otherwise agreed, be produced by the Supplier's Personnel within ten (10) days of completion of the Incident Response Services and sent to the Buyer.

4.3 Whilst the Supplier will use its reasonable endeavours to ensure that the same Supplier's Personnel will continue to be involved throughout the investigation of a particular incident during the Incident Response Services, it reserves the right to replace that Personnel.

4.4 The Supplier shall, where the Supplier's Personnel is present on the Buyer's premises, use all reasonable endeavours to ensure that the Supplier's Personnel complies with such reasonable site rules and procedures as are notified to the Supplier from time to time.

4.5 In the event that a level of security clearance is required in order to provide the Incident Response Services, The Supplier will use its reasonable endeavours to provide a Supplier's Personnel with the appropriate levels of security clearance. For the avoidance of doubt, if the Supplier is unable to provide Personnel with appropriate levels of security clearance, The Supplier will not be liable for any failure to perform or complete the Incident Response Services or delay in performing its obligations under the Order Contract.

5 Buyer's Duties

5.1 The Buyer agrees that due to the nature of the Retained Incident Response Services, the Supplier cannot guarantee that it will be able to perform and/or complete the Retained Incident Response Services. In particular, the Supplier may be unable to recover the data in whole or in part. In addition, the data recovered may not be of evidentially significant material, the Relevant Systems may suffer damage as a result

of the data recovery process and/or the Incident Response Services may result in loss of business operating time or interruption to service for the Buyer. Such problems cannot be identified by the Supplier until it has commenced the Incident Response Services and so the Buyer remains liable to pay the Charges notwithstanding the above (or such proportion of the Charges as the Supplier may determine in its absolute discretion).

5.2 The Buyer authorises the Supplier to work on or remove Relevant Systems which are compromised or which it believes to be compromised.

6 Charges and Expenses

6.1 The Annual Charges include Charges payable in respect of 5 days of Retained Incident Response Services for each Order Contract Year within the Term ("**Minimum Call Off Days**"). In the event the Buyer has not requested and used the Minimum Call-Off Days for a Order Contract Year in accordance with such process by the expiry of that Order Contract Year, then such Minimum Call Off Days shall roll forward (and continue to roll forward, where applicable) to the following Order Contract Year(s) and can be used by the Buyer during the Order Contract term. In the event the Buyer has not requested and used the Minimum Call-Off Days it is entitled to in each Order Contract Year throughout the Order Contract term by the end of such Order Contract term, such Minimum Call Off Days shall expire and cannot be used by the Buyer (and for the avoidance of doubt, the Buyer shall not be entitled to any refund of Charges in respect of the same).

6.2 If, in any Order Contract Year, the Buyer wishes to use one or more Minimum Call-Off Days applicable to future Order Contract Years, it may pull forward and use such Minimum Call-Off Days within that Order Contract Year. In such circumstances, the Minimum Call-Off Days for subsequent Order Contract Year(s) shall be reduced by the number of Minimum Call-Off Days brought forward. For the avoidance of doubt, for the purposes of clause 6.3 of this Annex, Charges in respect of any Minimum Call Off Days pulled forward shall be deemed Charges payable in respect of the period prior to termination.

6.3 If the Buyer wishes to purchase additional Retained Incident Response Services over and above the aggregate of the Minimum Call-Off Days permitted during the Term ("**Additional RIR Services**"), the Charges payable for such Additional RIR Services shall be calculated and invoiced at a rate of 90% of The Supplier's then current rates for Retained Incident Response Services as notified by The Supplier. Such Additional RIR Services shall be requested and approved in accordance with the process referred to in Section 3 above.

6.4 Unless otherwise stated in the relevant Response Proposal, the Charges do not include:

6.4.1 attendance by an The Supplier representative at any case conferences, meetings or court hearings or equivalent or the provision of any reports or information in connection with the same;

6.4.2 the storage by The Supplier of any property or data post completion of the Services;

6.4.3 and/or the cost of transporting the Relevant Systems to/from The Supplier's premises.

6.4.4 additional work which it transpires is necessary once the RIR Services have commenced but which are not listed in the Service Description or Response Proposal, including, but not limited to reverse engineering or additional work necessitated by a defect in any of the software or hardware included within the Relevant Systems.

If The Supplier agrees to carry out any of these activities it shall be entitled to charge reasonable additional Charges (subject to agreeing the same with the Buyer in advance).

6.5 All Retained Incident Response Services (including the Minimum Call-Off Days) are invoiced on the basis that work will be undertaken during Normal Office Hours. Any work carried out outside of Normal Office Hours will be charged at twice The Supplier's then current day rate.

6.6 The Supplier's Consultants record all time spent on an assignment including time spent travelling for the purposes of the assignment. Time is accounted for in units of half a day. No charge is made for periods when the Consultant is absent due to illness or holidays. As a worked example, if The Supplier was required to work from 9:00am until midnight on a Working Day, the rate would be two and half days.

6.7 To the extent that the Supplier is required to work outside Normal Office Hours, the Buyer shall be permitted to set-off any surcharge incurred in accordance with clauses 6.5.and 6.6 against any Minimum Call Off Days. For the avoidance of doubt, to the extent the Buyer does not have sufficient Minimum Call Off Days to satisfy the surcharge payable, The Supplier shall invoice the Buyer for any shortfall amount.

## Annex 2 (Remediate Services)

1 Definitions

"**Remediate Services**" (also known as "**Security Improvement Services**") means the Services as detailed in the Service Description (to the extent applicable) and Order Contract to improve the Buyer's resilience to cyber breaches or attacks and which may include assessing, identifying, prioritising and improving resilience to risks, breaches, threats, vulnerabilities or deficiencies in the System;

"**System**" means the systems and networks on or in relation to which the Buyer requires the Supplier to perform the Remediate Services as described in the Order Form, together with any software, systems, networks, premises, equipment, data, data structures, protocols, policies, processes, computers, hardware, firmware, linked to the same and data passing across or contained in any of the foregoing as well as premises owned, operated or controlled by the Buyer;

**"Business Operations Environment"** means the Systems and any other business operations impacted due to the performance of Remediate Services; and

"**Service Description**" means the service description applicable to the Remediate Services, as updated by the Supplier from time to time.

2 Buyer's Duties

2.1 The Buyer agrees, in addition to any obligations contained in the Service Description and the Order Form:

2.1.1 to work collaboratively with the Supplier to provide all relevant information in relation to its Business Operations Environment to the Supplier required to enable the Supplier to deliver the Remediate Services;

2.1.2 to obtain consent from any relevant third parties to enable the Remediate Services to be performed which may include (but is not limited to) its ISP and any third party suppliers of the Systems within Business Operations Environment and, when requested by the Supplier, to provide written evidence of such consent and, where relevant, to notify relevant employees that the Remediate Services have been scheduled;

2.1.3 to ensure that the Buyer has consent from the relevant parties to provide to the Supplier any report, findings data or information prepared by or in which a third party has any rights and for the Supplier to use the contents of such reports as necessary in the provision of the Remediate Services;

2.1.4 to arrange a mutually convenient time and date with the Supplier for the performance of the Remediate Services and, if necessary, to inform its ISP of the date agreed with the Supplier;

2.1.5 that it shall ensure the interim resilience of its entire Business Operations Environment during the performance of Remediate Services which should include amongst others (but not limited to) proper and full back-up of all data and copies of all, computer programs and data which are held immediately prior to commencement of the Remediate Services, and which may be affected by the provision of the Remediate Services and, where appropriate, regular performance of interim backups during the performance of the Remediate Services, to enable straightforward recovery and/or reinstatement of any and all data and/or computer programs lost or damaged (whether in whole or part) through provision of the Remediate Services;

2.1.6 to provide suitable working space for the consultant if the Remediate Services is to take place on the Buyer's premises, including a desk, network access and, where necessary to perform the Remediate Services, access to data centres, internal networks and systems including administrator level accesses where necessary, server rooms and/or switch rooms;

2.1.7 to ensure at least one employee who shall have substantial experience and knowledge of the Business Operations Environment and will act as liaison between the Buyer and the Supplier, responding promptly to any queries or requests for information;

2.1.8 to co-operate with the Supplier and to provide it with all information that is reasonably necessary and/or which it reasonably requests in a timely manner to enable the effective, safe and secure provision of the Remediate Services. Further, the Buyer shall facilitate access to all Business Operations Environment in a timely manner as required for the effective delivery of the Remediate Services;

2.1.9 to inform the Supplier of any organisational, policy, network, stakeholder, infrastructure and/or any other changes that may impact the Remediate Services or the Supplier's ability to provide the Remediate Services;

2.1.10 at all times to co-operate with the Supplier and to provide the Supplier promptly with such other relevant information in relation to the Business Operations Environment and appropriate log files about the Systems within Business Operations Environment, network, premises, equipment, data structures, protocols, software, hardware and firmware as is reasonably required by the Supplier;

2.1.11 to ensure that, where the Remediate Services are taking place on the Buyer's premises, the premises are safe. The Buyer will indemnify, keep indemnified and hold harmless The Supplier in full and on demand from and against all liabilities, losses, damages, claims, proceedings and legal costs, judgments and costs (including costs of enforcement) and expenses (in each case whether direct, indirect or consequential) which the Supplier (or its Affiliates) incurs or suffers arising out of or in connection with any claim or action against the Supplier for death and/or personal injury arising out of the Buyer's failure to provide safe premises;

2.1.12 that, in cases where the Supplier requires the Buyer to sign an Authorisation Form, by signing the Authorisation Form, the Buyer consents, for itself and on behalf of all its Affiliates, to the Supplier (or its Affiliates) performing the Remediate Services and confirms that it has procured, where necessary, the consent of all its (and its Affiliates') third party service providers (including ISPs), third party software vendors and equipment owners, employees, agents and sub-contractors for the Supplier (or its Affiliates) to carry out the Remediate Services. Such consent includes authorisation for the purposes of Section 3 of the Computer Misuse Act 1990 that the Supplier, its Affiliates and its and their employees (including, but not limited to, the Consultant), agents and sub-contractors may perform Remediate Services which may;

2.1.12.1 impair the operation of the Business Operations Environment;

2.1.12.2 hinder access to the Systems within Business Operations Environment; and

2.1.12.3 impair the operation of any program and/or the reliability of any data relating to the Systems within Business Operations Environment;

2.1.13 that, whilst the Supplier will use reasonable endeavours and Good Industry Practice to avoid disruption of the Buyer's network, disruption to the Buyer's Business Operations Environment and/or possible loss of or corruption to data and/or software or business interruption (including but not limited to disruption in operation of business units, and/or resource coordination or any disruption arising out of Buyer`s failure to ensure that interim resilience of Business Operations Environment as set out in clause 3.1.5) or any events of a similar nature may occur, and the Buyer agrees to make back-ups pursuant to clause 2.1.5;

2.1.14 to notify the Supplier in writing in advance after becoming aware of any periods during which the Supplier should not perform the Remediate Services or should cease performing the Remediate Services due to business interruption, organisational changes affecting the operation of Business Operations Environment, and/or critical business processes (such as batch runs) or if any part of the Business Operations Environment is business critical so that the Supplier may, if necessary, with the Buyer's consent, modify its approach. The Buyer shall advise the Supplier of any change control policies or processes which may be relevant to the Services and shall ensure that any necessary escalations and/or prioritisations are obtained to enable the Supplier to able to provide the Services without impediment;

2.1.15 that, where the Supplier (or its Affiliates) supplies any software and/or hardware as part of the Remediate Services, Buyer shall only use such software and/or hardware for lawful purposes, solely to the extent necessary to receive the benefit of the Remediate Services and in accordance with any applicable licence terms and the Supplier's (or its Affiliates') instructions provided from time to time; and

2.1.16 the Buyer shall assume all liability and shall indemnify, keep indemnified and hold harmless the Supplier, its Affiliates and its and their officers, employees, agents, contractors and sub-contractors in full and on demand from and against any and all third party claims (including claims for alleged or actual infringement of Intellectual Property Rights), losses, damages, demands, costs, expenses, fees (including court and legal fees) and liabilities (in each case whether direct, indirect or consequential) of whatever nature suffered, incurred or sustained by the Supplier (or its Affiliates) as a result of the provision of the Remediate Services, save to the extent that any such losses, damages, demands, costs, expenses, fees or liabilities are incurred as a direct result of the Supplier's breach of the Contract.

3 Liability

3.1 The Buyer acknowledges that there is a risk that the Remediate Services may lead to business interruption, inability to access other services, loss of use, failure to store or transmit any data or other information and/or communication in the Business Operations Environment, as well as other tangible and/or intangible losses, the loss or corruption of the Buyer's data and/or Personal Data affected by the Remediate Services, and that the same is an inherent risk of Remediate Services even when performed in accordance with Good Industry Practice. The Buyer is advised to back up its data and ensure the internal resilience of the Business Operations Environment prior to the Start Date and during the Remediate Services as described in clause 3.1.5. Subject to clause 11.4 of the Core Terms (DPS), the Supplier will not be liable for any such loss of data, any loss due to business interruption in the Business Operations Environment and any other losses set out in this clause 3.1 as well as loss of profit, or revenues, incidental and /or indirect and consequential losses.

3.2 Due to the nature of the Remediate Services, the Supplier cannot and does not provide any guarantee or warranty that: (i) the Supplier will identify all risks, breaches, threats, vulnerabilities and/or deficiencies that relate to the Business Operations Environments, networks, software or devices that are subject to the Remediate Services; and (ii) the Remediate Services will ensure that the Buyer's systems, networks, software or devices will cease to be vulnerable, susceptible to exploitation or protected from all attacks, breaches or hacks or threats or impacts resulting from the acts or omissions of authorised users of the Business Operations Environment.

3.3 Subject to clause 11.4 of the Core Terms (DPS), the Supplier excludes its liability for non-performance of the Remediate Services and breach of contract to the extent that the Supplier is unable to perform the Remediate Services as a result of those matters detailed in clause 2.1 above or the Buyer not fulfilling their obligations in relation to the Order Contract.

3.4 The Buyer acknowledges that, Subject to clause 11.4 of the Core Terms (DPS), the Supplier shall not be liable for any cyber threats and or attacks that occur in the Buyer's Business Operations Environment before, during or after the delivery of the Remediate Services, including cyber threats and/or attacks that occur due

to any changes that the Buyer makes to their Business Operations Environment, during or after the delivery of the Remediate Services.

# 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"**)<br>And<br>**[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:<br>• **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] | |
| Financial variation: | Original Contract Value: | £ **[insert** amount] |
| | Additional cost due to variation: | £ **[insert** amount] |
| | New Contract value: | £ **[insert** amount] |

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

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

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

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

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

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

# Joint Schedule 3 (Insurance Requirements)

## 1. The insurance you need to have

1.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

1.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

1.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

1.2 The Insurances shall be:

1.2.1 maintained in accordance with Good Industry Practice;

1.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

1.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

1.2.4 maintained for at least six (6) years after the End Date.

1.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

## 2. How to manage the insurance

2.1 Without limiting the other provisions of this Contract, the Supplier shall:

2.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

2.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

2.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other

evidence of placing cover representing any of the Insurances to which it is a party.

## 3. What happens if you aren't insured

3.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

3.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

## 4. Evidence of insurance you must provide

4.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

## 5. Making sure you are insured to the required amount

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

## 6. Cancelled Insurance

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

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

## 7. Insurance claims

7.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to claim under any of the Insurances. In the event that the Relevant Authority

receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

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

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

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

### ANNEX: REQUIRED INSURANCES

**1.** The Supplier shall hold the following [standard] insurance cover from the DPS Start Date in accordance with this Schedule:

1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than 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)

## 2. What is the Commercially Sensitive Information?

2.1 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.

2.2 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).

2.3 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 | 11 April 2023 | Breakdown of service costs | Term of the Order Contract (including any extensions) |
| 2 | 11 April 2023 | Breakdown of staff costs | Term of the Order Contract (including any extensions) |

# Joint Schedule 10 (Rectification Plan)

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

| | | | |
|---|---|---|---|
| Steps taken to prevent recurrence of Default | **Steps** | **Timescale** | |
| | 1. | [date] | |
| | 2. | [date] | |
| | 3. | [date] | |
| | 4. | [date] | |
| | […] | [date] | |
| Signed by the Supplier: | | Date: | |
| **Review of Rectification Plan** [CCS/Buyer] | | | |
| Outcome of review | [Plan Accepted] [Plan Rejected] [Revised Plan Requested] | | |
| Reasons for Rejection (if applicable) | [**add** reasons] | | |
| Signed by [CCS/Buyer] | | Date: | |

# Joint Schedule 11 (Processing Data)

**Status of the Controller**

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

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

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

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

(d) "Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

## Where one Party is Controller and the other Party its Processor

2. Where a Party is a Processor, the only processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

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

4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

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

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

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

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

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

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

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

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

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

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

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

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

6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

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

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

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event; and/or

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

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

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

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

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

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

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

(b) obtain the written consent of the Controller;

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

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

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

14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

**Where the Parties are Joint Controllers of Personal Data**

16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

**Independent Controllers of Personal Data**

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

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

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

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

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

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

22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

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

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

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

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

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

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

25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data A) Template

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

1.1 The contact details of the Relevant Authority's Data Protection Officer are: dataprotectionofficer@ukhsa.gov.uk

1.2 The contact details of the Supplier's Data Protection Officer are: Joy Evans, dataprotection@nccgroup.com

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

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

| **Description** | **Details** |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:<br><br>• Information regarding UKHSA staff including volunteers, agents, temporary workers, which may include sensitive personal data<br>• Data for which UKHSA is the controller<br>• Other data supplied to UKHSA under collaboration agreements for which it is the controller<br>Members of the public (where data about them is held by UKHSA as controller) |
| Duration of the Processing | The duration of processing is 12 months in the first instance, extendable by two further 12 month periods at the option of UKHSA.<br><br>The processing will start from the commencement date of the contract as referenced in section 1 |
| Nature and purposes of the Processing | The collection, storage, retrieval, analysis, and consultation of data from IT systems operated by UKHSA, which may include IT system data, personal usage patterns, software usage patterns, data entered and processed within UKHSA IT infrastructure |

| | |
|---|---|
| | For the purposes of acceptable use compliance, disciplinary processes, the detection and management of cyber security events and incidents, cyber security incident response management, regulatory and statutory compliance, the detection and prevention of crime.<br><br>Where necessary, information gathered as part of this contract may be disclosed to other parts of UKHSA (for example as part of disciplinary investigations), auditors and legal counsel, wider UK government, and if requested law enforcement agencies within the United Kingdom. Information disclosure to third parties will be governed by UKHSA corporate policies. |
| Type of Personal Data | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*<br><br>• Primarily system usage data including use attributed to individual user identities, either at rest or being transmitted, including but not limited to:<br>  ○ Usage patterns and anomaly detection<br>  ○ IP addresses<br>  ○ Geographical location including user geographical location<br>  ○ Websites accessed including full URLs<br>  ○ System-derived meta-data including file names, file attributes, file checksums<br>  ○ Content matching against industry-standard indicators, signatures and tokens<br>• Data of any format within UKHSA IT infrastructure (primarily in incident response), either at rest or being transmitted, including but not limited to:<br>  ○ Names<br>  ○ Addresses<br>  ○ Dates of birth<br>  ○ Salary and pay data<br>  ○ Images |
| Categories of Data Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*<br><br>• Staff, including volunteers, agents and temporary workers |

| | |
|---|---|
| | • Customers/clients, including those accessing UKHSA public services e.g. via the Internet<br>• Suppliers<br>• Medical/Patient/NHS data<br>• Other data supplied to UKHSA under collaboration agreements<br>• Members of the public (where data about them is held by UKHSA)<br>• Users of UKHSA IT Infrastructure |
| Plan for return and destruction of the data once the Processing is complete<br>UNLESS requirement under Union or Member State law to preserve that type of data | Data retention within UKHSA managed systems accessed by the Supplier is configured by UKHSA to meet UKHSA retention requirements and is under the control of UKHSA.<br><br>Data that is copied to the Supplier will only be retained by the Supplier for as long as it is needed for the fulfilment of their processing obligations under contract, and in default will be deleted at contract end by the supplier. |

## B) DPS Contract Personal Data Processing

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **UKHSA is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, UKHSA 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<br>i. Ensuring effective communication between the Supplier and CSS<br>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:<br>i. Contact details of, and communications with, UKHSA staff concerned with management of the DPS Contract<br>ii. Contact details of, and communications with, Buyer staff concerned with award and management of Order Contracts awarded under the DPS Contract,<br>iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract<br>Contact details, and communications with Supplier staff concerned with management of the DPS Contract |
| Categories of Data Subject | Includes:<br>i. UKHSA staff concerned with management of the DPS Contract<br>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<br><br>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 – Not applicable**

# Order Schedule 2 (Staff Transfer)

## Definitions

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

**"Employee Liability"** all claims, actions, proceedings, orders, demands, complaints, investigations (save for any claims for personal injury which are covered by insurance) and any award, compensation, damages, tribunal awards, fine, loss, order, penalty, disbursement, payment made by way of settlement and costs, expenses and legal costs reasonably incurred in connection with a claim or investigation including in relation to the following:

a) redundancy payments including contractual or enhanced redundancy costs, termination costs and notice payments;

b) unfair, wrongful or constructive dismissal compensation;

c) compensation for discrimination on grounds of sex, race, disability, age, religion or belief, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation or claims for equal pay;

d) compensation for less favourable treatment of part-time workers or fixed term employees;

e) outstanding debts and unlawful deduction of wages including any PAYE and National Insurance Contributions in relation to payments made by the Buyer or the Replacement Supplier to a Transferring Supplier Employee which would have been payable by the Supplier or the Sub-contractor if such payment should have been made prior to the Service Transfer Date and also including any payments arising in respect of pensions;

| | |
|---|---|
| | f) claims whether in tort, contract or statute or otherwise;<br><br>any investigation by the Equality and Human Rights Commission or other enforcement, regulatory or supervisory body and of implementing any requirements which may arise from such investigation; |
| **"Former Supplier"** | a supplier supplying the Deliverables to the Buyer before the Relevant Transfer Date that are the same as or substantially similar to the Deliverables (or any part of the Deliverables) and shall include any Sub-contractor of such supplier (or any Sub-contractor of any such Sub-contractor); |
| **"Partial Termination"** | the partial termination of the relevant Contract to the extent that it relates to the provision of any part of the Services as further provided for in Clause 10.4 (When CCS or the Buyer can end this contract ) or 10.6 (When the Supplier can end the contract); |
| **"Relevant Transfer"** | a transfer of employment to which the Employment Regulations applies; |
| **"Relevant Transfer Date"** | in relation to a Relevant Transfer, the date upon which the Relevant Transfer takes place, and for the purposes of Part D: Pensions, shall include the Commencement Date, where appropriate; |
| **"Supplier's Final Supplier Personnel List"** | a list provided by the Supplier of all Supplier Personnel whose will transfer under the Employment Regulations on the Service Transfer Date; |
| **"Supplier's Provisional Supplier Personnel List"** | a list prepared and updated by the Supplier of all Supplier Personnel who are at the date of the list wholly or mainly engaged in or assigned to the provision of the Services or any relevant part of the Services which it is envisaged as at the date of such list will no longer be provided by the Supplier; |

| | |
|---|---|
| **"Staffing Information"** | in relation to all persons identified on the Supplier's Provisional Supplier Personnel List or Supplier's Final Supplier Personnel List, as the case may be, such information as the Buyer may reasonably request (subject to all applicable provisions of the Data Protection Laws), but including in an anonymised format:<br>(a) their ages, dates of commencement of employment or engagement, gender and place of work;<br>(b) details of whether they are employed, self-employed contractors or consultants, agency workers or otherwise;<br>(c) the identity of the employer or relevant contracting Party;<br>(d) their relevant contractual notice periods and any other terms relating to termination of employment, including redundancy procedures, and redundancy payments;<br>(e) their wages, salaries, bonuses and profit sharing arrangements as applicable;<br>(f) details of other employment-related benefits, including (without limitation) medical insurance, life assurance, pension or other retirement benefit schemes, share option schemes and company car schedules applicable to them;<br>(g) any outstanding or potential contractual, statutory or other liabilities in respect of such individuals (including in respect of personal injury claims);<br>(h) details of any such individuals on long term sickness absence, parental leave, maternity leave or other authorised long term absence;<br>(i) copies of all relevant documents and materials relating to such information, including copies of relevant contracts of employment (or relevant standard contracts if applied generally in respect of such employees); and |

| | |
|---|---|
| | (j) any other "employee liability information" as such term is defined in regulation 11 of the Employment Regulations; |
| **"Term"** | the period commencing on the Start Date and ending on the expiry of the Initial Period or any Extension Period or on earlier termination of the relevant Contract; |
| **"Transferring Buyer Employees"** | those employees of the Buyer to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date; |
| **"Transferring Former Supplier Employees"** | in relation to a Former Supplier, those employees of the Former Supplier to whom the Employment Regulations will apply on the Relevant Transfer Date and whose names are provided to the Supplier on or prior to the Relevant Transfer Date. |

## INTERPRETATION

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

## Which parts of this Schedule apply

Only the following parts of this Schedule shall apply to this Order Contract:

- *Part C (No Staff Transfer On Start Date)*
- *Part D (Pensions) ]*
    - *N/A*

# PART A: STAFF TRANSFER AT THE START DATE

# OUTSOURCING FROM THE BUYER – NOT APPLICABLE

# PART B: STAFF TRANSFER AT THE START DATE

# TRANSFER FROM A FORMER SUPPLIER ON RE-PROCUREMENT – NOT APPLICABLE

# PART C: NO STAFF TRANSFER ON THE START DATE

## 1. What happens if there is a staff transfer

The Buyer and the Supplier agree that the commencement of the provision of the Services or of any part of the Services will not be a Relevant Transfer in relation to any employees of the Buyer and/or any Former Supplier.

Subject to Paragraphs 0, 0 and 0, if any employee of the Buyer and/or a Former Supplier claims, or it is determined in relation to any employee of the Buyer and/or a Former Supplier, that his/her contract of employment has been transferred from the Buyer and/or the Former Supplier to the Supplier and/or any Sub-contractor pursuant to the Employment Regulations then:

1.1.1 the Supplier will, within 5 Working Days of becoming aware of that fact, notify the Buyer in writing;

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

1.1.3 if such offer of employment is accepted, the Supplier shall immediately release the person from its employment;

1.1.4 if after the period referred to in Paragraph 1.1.2 no such offer has been made, or such offer has been made but not accepted, the Supplier may within 5 Working Days give notice to terminate the employment of such person;

and subject to the Supplier's compliance with Paragraphs 1.1.1 to 1.1.4:

(a) the Buyer will indemnify the Supplier and/or the relevant Sub-contractor against all Employee Liabilities arising out of the termination of the employment of any of the Buyer's employees referred to in Paragraph 0; and

(b) the Buyer will procure that the Former Supplier indemnifies the Supplier and/or any Sub-contractor against all Employee Liabilities arising out of termination of the employment of the employees of the Former Supplier referred to in Paragraph 0.

The indemnities in Paragraph 0 shall not apply to any claim:

1.1.5 for discrimination, including on the grounds of sex, race, disability, age, gender reassignment, marriage or civil partnership, pregnancy and maternity or sexual orientation, religion or belief or equal pay or compensation for less favourable treatment of part-time workers or fixed-term employees in relation to any alleged act or omission of the Supplier and/or Sub-contractor; or

1.1.6 any claim that the termination of employment was unfair because the Supplier and/or any Sub-contractor neglected to follow a fair dismissal procedure

The indemnities in Paragraph 0 shall not apply to any termination of employment occurring later than 3 Months from the Commencement Date.

If the Supplier and/or the Sub-contractor does not comply with Paragraph 0, all Employee Liabilities in relation to such employees shall remain with the Supplier and/or the Sub-contractor and the Supplier shall (i) comply with the provisions of Part D: Pensions of this Schedule, and (ii) indemnify the Buyer and any Former Supplier against any Employee Liabilities that either of them may incur in respect of any such employees of the Supplier and/or employees of the Sub-contractor.

**Limits on the Former Supplier's obligations**

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

# PART D: PENSIONS NOT APPLICABLE

# Part E: Staff Transfer on Exit – Not applicable

# Order Schedule 4 (Order Tender)

MDR Services will be delivered in accordance with the following Statement of Work. For the purposes of this Order Contract, words “MDR” and “XDR” are used interchangeably and have the same meaning

## 1 Statement of Work

## 1.1 Between:

UK Health Security Agency (a UK Governmental organisation, part of the Department of Health and Social Care) ("UKHSA" or the “Client” or the “Buyer”); and:
NCC GROUP SECURITY SERVICES LIMITED (a company registered in England and Wales, with number 04474600) whose registered office is at XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, England, M3 3AQ ("NCC Group" or the “Supplier”).

## 1.2 Background:

This Statement of Work sets forth the parameters, pricing, specifications, and any additional terms applicable to the provision of the Services and Deliverables referred to in this Statement of Work. The combination of the terms of the Call-Off Contract and the provisions of this Statement of Work shall together constitute the agreement between the Parties in respect of the XDR Services to be provided hereunder.

Terms not otherwise defined in this Statement of Work shall have the meanings set out in the Call-Off Contract. In the event of any conflict between the terms of this Statement of Work and the Call-Off Contract, the terms in this Statement of Work shall govern.

### 1.2.1 Additional Definitions

**Consultants** – These will be NCC Group or its affiliates permanent employees delivering the services.
**Log Source Inventory** – The agreed listing of all Log Source(s) that are required to be collected and processed by the Managed SIEM service which will be jointly agreed between the parties and maintained over the life of the service as contained at Appendix 1.
**ITSM** – IT Service Management. NCC Group utilise ServiceNow
**XDR** – Managed Extended Detection and Response services as provided by NCC Group in accordance with this Statement of Work
**XDR Lite** – Microsoft 365 Defender coverage only XDR Service

**MDE** – Microsoft Defender for Endpoint
**SIEM** – Security Information and Event Management
**SOC** – Security Operations Centre, being NCC Group's Security Operations centre, located in UK, Netherlands and/or Australia.
**SoW** – Statement of Work
**RIR** – Retained Incident Response

### 1.2.2 Confidentiality Notice

This Statement of Works has been prepared exclusively for the Client and contains information that should be considered the confidential property of NCC Group or the Client.

NCC Group gives permission to the Client to copy this Statement of Works for the purposes of disseminating information: (i) internally within the Client and its Affiliates (including to its and their officers and employees, professional advisers or consultants, contractors and sub-contractors) and/or (iii) to any other body where the Client is required to do so by applicable law or regulation or by an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction. Other than as permitted by the foregoing, this Statement of Works must not be disclosed to any third party.

### 1.2.3 Data Processing

| Services Provided by NCC Group | Included within this Statement of Works |
|---|---|
| SOC Services Delivered from the following location | UK |
| SOC Platform Data Storage & Processing Location(s) | Data is stored in the client's tenant and may be processed in the UK |
| XDR Managed Endpoint (Endpoint XDR) **Using Microsoft Defender for Endpoint Plan 2** | ✓ |

Any data processed by NCC Group and/or Azure will be processed in the UK. Although this is primarily alert and meta-data from your XDR services, some of the contents of those alarms and meta-data could constitute personal data in certain circumstances.

**IMPORTANT INFORMATION**

- The provisioning, payment and maintenance of any Microsoft licenses or subscriptions which are required to enable the provision of the Services are

solely the responsibility of the Client. This includes ingestion charges and storage costs.
- All Microsoft licensing and subscriptions are outside the scope of the Services.

## 2 Services Covered Within This SoW

This section defines the specifics of the Services to be delivered to UKHSA:

# 2.1 XDR Service with 24x7 SOC

- XDR service for up to 250GB/Day Microsoft Sentinel Log Consumption during this service agreement.
    - Year 1: Up to 250GB/Day Microsoft Sentinel Log Consumption
    - Optional Year 2: Up to 250GB /Day Microsoft Sentinel Log Consumption
    - Optional Year 3: Up to 250GB/Day Microsoft Sentinel Log Consumption
- Design, deployment, and management of one **Microsoft Sentinel Service Workspace.**
- Onboarding of Data sources as defined within the Log Source Inventory. Data sources identified as candidates for the Log Source Inventory at this time are:
    - Azure Active Directory Connector (Requires AAD P2 license)
    - Azure Active Directory Identity Protection (Requires AAD P2 license)
    - Azure Activity Logs
    - Microsoft Defender for Cloud (Requires ASC at Standard Tier)
    - Microsoft Defender for Endpoint
    - Other assets up to a logging level defined in the agreed Log Source Inventory.
- Preview features and preview data connectors are not subject to inclusion within the Service Level Agreement for monitoring. Although Microsoft provide a large selection of data connectors in both preview and GA, this does not guarantee that detection logic and alerting is available by default. Should any custom detection logic, or alerting be required, this is a chargeable engagement.
- 32 days professional services for the deployment of service components, or the validation of pre-existing configurations. This also includes the on boarding and managed service take on. Validation and testing is also included within this allocation of professional services time, to ensure all applicable coloration logic is verified.
- NCC Group Managed Endpoint XDR for 25,000 endpoints:

    - Endpoint Managed Service component for Microsoft Defender for Endpoint
    - Support for UKHSA during the onboarding phase of the project
    - Onboarding of the deployed endpoint agents into the service
    - Remote remediation support including the ability to contain or quarantine an endpoint if authorised by UKHSA.

  - Completion of the Endpoint XDR approved response process. Thereby authorising NCC Group to isolate endpoints based on pre-approved activities.
  - Correlation of alerts across the XDR service to identify security incidents.

- **24x7x365 SOC** monitoring of security events from the Log Source Inventory to identify potential malicious activity.
  - Triage of security events, including classifications of alerts/incidents against business criticality.
  - Please note, our analysts will not provide support and remediation advice for low and informational incidents and this data will be retained for forensic purposes only.

- Provision of security incident remediation recommendations when alerts/incidents are identified
  - NCC Group SOC will respond to all alerts raised within the NCC Group ITSM portal, working with the Client to action all associated tickets in ITSM.
  - Engagement with UKHSA when security events require validation and/or response

- Threat Hunting
  - scheduled 'Threat Hunts' to identify attempts to bypass or evade the detection capabilities of existing rules and analytics.
- Access to the NCC Group ServiceNow platform API will be provided.
- Term – 1 Year with an optional second and third year. Please refer to the invoicing profile in Section 4.4 for payment terms.

## 2.2 Clarification

- Microsoft Subscription not included in this managed service.
- Defender for Endpoint Plan 2 is a premium Microsoft tool designed for EDR and is required for the delivery of this managed service. The free Microsoft Defender AV solution is not suitable and should not be confused with Defender for Endpoint.

## 2.3 Related Documentation

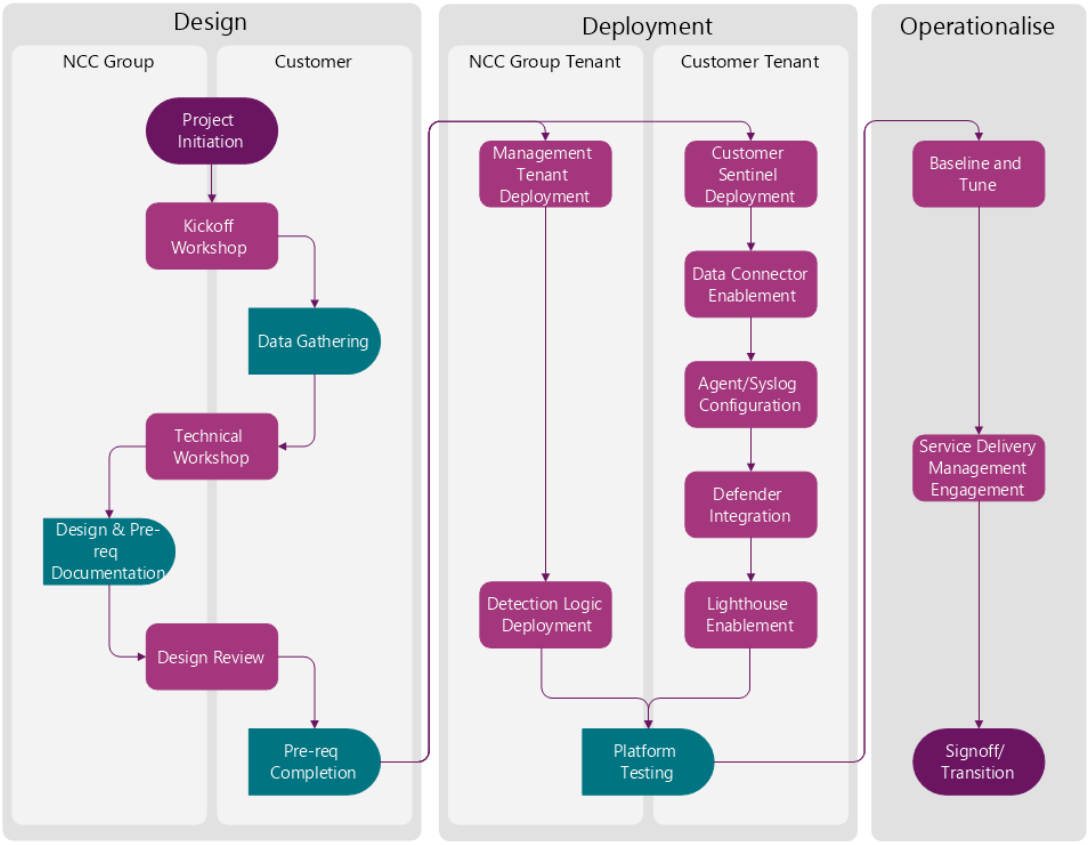
In addition to the Agreement, this section should be read in conjunction with NCC Group's **Managed Detection and Response Service Description and SLA** document. Within the Service Description and SLA document, refer to **Section 5 – SIEM Threat Detection Service** for the description of the general principles of the Service and **Section 10 – MDR Service Levels and Service Credits section** which defines the applicable Service Levels (each of these documents, the "**Appendices**").

## 2.4 Setup Services

This section describes the activities carried out by NCC Group during the onboarding process.

# 2.5 Onboarding Process

The following process will be completed as part of the implementation of the XDR service.




### 2.5.1 Element Breakdown

#### *2.5.1.1 Project Initiation*

The purpose of the project initiation call is to introduce the project management team, technical resources and to give a high-level overview of the project plan. The project initiation call will result in all parties involved understanding the high-level project workflow and milestones, as well as any prospective dates/location for the use case workshop.

#### *2.5.1.2 Remote Content Workshop*

The purpose of the content workshop is to perform a discovery exercise to identify the key areas and/or risks that the Client wishes to secure/mitigate with the Managed Service. This workshop is fully interactive; information discovered in this workshop is used to build the content profile that will be implemented by the NCC Group SIEM Consultant. The use case workshop will result in the creation of the threat detection profile. From this documentation pack, the SIEM consultant is provided with intelligence that is to be used to build the content that is to be monitored.

#### *2.5.1.3 Escalation Matrix*

The purpose of the escalation matrix documentation is to record the escalation tree that the SOC will use in the event of an incident. This documentation records the primary,

secondary and tertiary contacts that are to be used in line with the priority matrix contained within the standard service description. Completion of the escalation matrix documentation will provide the SOC with the relevant contact information that is to be used in the event of security incidents at each severity level.

#### *2.5.1.4 Secure Portal Access Provisioning*

The purpose of the portal access provisioning task is to provide the appropriate Client contacts with access to the NCC Group Secure portal. This system is used for the secure transmission of incident details, documentation and method of communication between the NCC Group SOC and the Client.

Completion of this task will result in a list of provisioned Client accounts. All recipients of an account will receive a setup email with user guide. Additional accounts can be requested post-project via a ticket on the secure portal.

#### *2.5.1.5 Access requirements*

**Initial deployment**: The Client is required to run a custom PowerShell script to grant temporary permissions within their Azure Tenant. The script will create a Service Principal with Global Administrator and Security Administrator group membership within Azure Active Directory. The script will also grant temporary Role Based Access Control (RBAC) 'owner' permissions to either the Client's Sentinel-specific or primary subscription. These permissions are required for the initial infrastructure roll out and can be removed when completed.

**Permanent access:** Ongoing access will be provisioned through Azure Lighthouse, which provides access to the Client's log analytics workspace. An application registration with rights to read M365 Defender data is also created and retained. The Client is required to set up analysts as guests within their Microsoft Defender for Endpoint account.

**Subscription options**: The deployment can be made to the Client's primary subscription or to a separate Sentinel subscription in the same tenant. The second option would avoid the service principal having access to other resources on the Client's primary subscription.

#### *2.5.1.6 Data On Boarding (as appropriate)*

The purpose of the data on boarding task is to configure the collection mechanisms used to ingest data into the Managed SIEM platform from the log sources determined during the scoping phase. Logs will be collected from network devices, servers, intrusion detection systems as well as any other source types defined as in scope in the Log Source Inventory. Completion of this task will result in the functional collection of logs/events from all in- scope log sources.

#### *2.5.1.7 Content Implementation*

The purpose of the data use case implementation task is to configure the detection profile. During this task, it may be necessary for the NCC Group SIEM consultant to work alongside Client technical contacts to ensure that the log sources are logging at an appropriate level to fulfil a use case. Completion of this task will result in the functional implementation of the appropriate NCC Group curated threat detection profile.

#### *2.5.1.8 Baselining*

The purpose of the baselining phase is to ensure that the implemented threat detection profile is tuned to an acceptable level and that an excessive number of incidents are not raised once the service has been transitioned to live. During baselining, a dedicated SOC Analyst will raise tickets via the secure portal to work with the Client to tune the use cases. All alerts will be processed through the SOC while baselining and tuning/optimisation occurs. The result of this task will be the effective tuning of the threat detection profile for real-time alerting in to the SOC, ensuring an effective signal to noise ratio.

#### *2.5.1.9 Baselining Timeline*

**Phase 1** - Initial baselining is undertaken by the assigned XDR Technical Delivery Consultant (XDR-TD). Approval of phase 1 is to be granted by XDR Technical Delivery Management prior to commencement of the next phase.
The success criteria of phase 1 will be measured through the removal of obvious misconfigurations and excessively triggering analytics (inc. false positives) that are a result of engineering workstreams (ie. lack of data, field mapping). Phase 1 will focus on the following key areas:
1. Top 5 triggered analytics.
2. Analytics triggered due to engineering workstreams and/or misconfiguration.

**Phase 2** - Second stage of baselining is conducted by the Analytics Development Team (ADEV). Approval of phase 2 is to be granted by ADEV Management prior to commencement of the next phase.
The success criteria of phase 2 will be measured through specific tuning recommendations and changes to (global) base analytics. Phase 2 will focus on the following key areas:
1. Remaining top 10 triggering analytics.
2. Analytics triggering due to nuances in the base analytics

**Phase 3** - Third stage of baselining is conducted by SOC. Approval of phase 3 is to be granted by SOC Management prior to the service / product going 'live' and entering BAU operations.
The success criteria of phase 3 will be measured through tuning, reducing the volume of false positive alerts to an acceptable level that will not adversely impact SOC operations, and a level at which tuning can be continued as part of the BAU managed service.

#### *2.5.1.10 Timeline for implementation*

The timeline will be provided in detail as part of the Project Initiation phase and is subject to change dependent upon circumstances outside of the control of NCC Group. The following dates are provided as estimated completion dates for the Set-up Services and the anticipated Go Live Milestones for the Services:

Estimated Go Live Milestone – XDR Service with 24/7 SOC

#### *2.5.1.11 Service Initiation*

The purpose of the service initiation task is to ensure that all project tasks have been completed successfully and to ensure that all documentation including the on-boarding

document, incident management process, UKHSA escalation matrix, and the agreed incident management policy, is accurate and implemented. Also discussed is the evolution of the service, and how the Client can request additional dashboards and reports to be created. The result of this task will be the sign-off and confirmation of the Go Live Milestone(s).

#### *2.5.1.12 ITSM (ITSM) Integration*

By default, Clients will be onboarded onto NCC Group's ITSM platform as part of the Service. ITSM is a dedicated workflow and case management system for NCC Group's managed services analysts and Clients.

API documentation to use external systems can be provided at the Client's request however, the Client is responsible for the integration work without NCC Group involvement.

The current information relating to the API integration can be provided upon request.

## 2.6 Retained Incident Response Services (RIR)

NCC Group's Retained Incident Response Services provide UKHSA with 24/7, 365, actionable and prompt support when a cyber security incident happens. The XDR Retained Incident Response Service ensures a continuity of service and full audit trail from alert analysis and threat hunting in the SOC to remote and on-site resource for incident response and forensic investigation by the Cyber Incident Response Team.

- Delivery of an incident response service on demand – XDR Standard
- Single Incident Response Escalation Process
- Availability of Incident Response consultants on a 24x7/365 basis.
- Defined response times for review of initial incident information and a consultant attending site.
- 5 Days of retained incident response call-off days included. (per year, or for the duration of the Term as detailed below)
- Term – 1 Year, with an optional second and third years from the relevant Go Live Milestone

**This section should be read in conjunction with** NCC Group's **Managed Detection and Response Service Description and SLA** document and in particular **Section 7 – MDR Retained Incident Response** which describes the general principles of the service and **Section 10 - MDR Service Levels and Service Credits section**) which defines the applicable Service Levels.

- The XDR Retained Incident Response (RIR) service – XDR Standard
- RIR will provide a continuity of service and audit trail from Alert Analysis and Threat Hunting in the SOC to remote and on-site forensic investigation by the CIRT team.
- The SOC Security analysts will provide remote support where required to advise on containment/remediation and provide guidance on ensuring non-recurrence of the incident. This remote support service is included in standard SOC escalation framework for up to 2 hours. Any further investigation after

such 2-hour window will require the activation of the Retained Incident Response Services.

- The Retained Incident Response Services aims to provide availability of a Security Consultant from the NCC Group CIRT team to commence remote and on-site forensic analysis of the incident in accordance with the applicable Target Service Levels.
- Should the SOC deem that the Retained Incident Response Service should be initiated for a Client, the SOC will contact the agreed point of escalation within the Client organisation to advise accordingly and request authorisation for the use of Incident Response consultancy days. Upon receipt of the approval from the Client to proceed with the Retained Incident Response service in respect of such Incident, the SOC shall pass such Incident to CIRT for the commencement of further investigation.

### 2.6.1 Service Level Details

| Service | XDR Standard Retainer |
|---|---|
| **On boarding conducted** | As part of the XDR Service |
| **Access to dedicated 24/7 telephone line** | ☑ |
| **Global IR personnel on standby 24/7 365** | ☑ |
| **SLA for Response (Mon- Sunday 24 hours)** | ☑ |
| ▪ **Telephone** | 3 hours |
| ▪ **Remote**** | 12 hours |
| ▪ **Onsite support (UK, EU, NA, APAC)** | 24 hours |
| ▪ **In transit (RoW)** | Best Endeavours |
| **Triage time Included** | Taken from Pre-paid budget |
| **Preferential access to Regulatory and privacy practitioners** | ☑ |

**Standard Incident Response is being provided pursuant to this Statement of Works.**

#### *2.6.1.1 Pre-paid Incident Response Days Terms*

- NCC Group may use reasonable endeavours to prioritise the scheduling of incident response services for those clients who have live incident response retainers with NCC Group, provided that any failure by NCC Group to meet the SLAs as a result of such prioritisation will not prejudice the UKHSA's ability to claim service credits.
- 5 Days of retained incident response call-off days included. These can be used for the duration of the 1 Year, with an optional second and third year, service agreement.

- All pricing is offered on the basis that work will be undertaken during normal office hours:
    - UK: (Monday to Friday - 0900 to 1730
- Any work carried out:
    - between 1800 and 0000 (midnight) on a Business Day will be charged at one-and-a half times the day rate;
    - between 0000 (midnight) and 0830 the next Business Day will be charged at twice the day rate; on Bank Holidays will be charged at twice the day rate.
- Any work carried outside these hours will be charged at twice the hourly rate.
- If UKHSA wish to purchase further hours for incident response in addition to the hours allocated within this agreement, NCC Group will charge this at the appropriate tier rate. If NCC Group incident response services are called upon outside of this agreement, then the appropriate standard rate will apply.
- Throughout the delivery of this retainer, NCC Group will work closely with you to ensure that we have a clear understanding of your requirements and can help you to address these as they arise.
- The retainer covers one entity only, unless specified in the scope. An entity is defined by either one legal entity and /or one organisation with one set of incident response policies & procedures and/or one incident response team who will oversee all incident response activity.
- All unused RIR days will be considered as spent having been available for the duration of the service agreement.

All timelines specified above are to be calculated from the date of signature by UKHSA of this Statement of Works unless specified otherwise.

## 2.7 Service Boundaries, Dependencies and Assumptions

The following section outlines features that are not in scope of the standard service offering:

- **The provisioning and payment for, and maintenance of, any Microsoft license subscriptions required to enable the Services to be delivered is solely the responsibility of the client. This includes ingestion charges and storage costs. All Microsoft licensing and subscriptions are outside the scope of the service offered by NCC Group.**
- The Client shall supply contact details for a primary contact, who will communicate on a regular basis with NCC Group regarding any matter arising

in connection with the operation and provision of the service to be provided by NCC Group. This includes any projected increases in, or abnormal usage of, the service outside the established and agreed parameters in the commercial proposal.

- Preview features and connectors are not subject to inclusion within the Service Level Agreement for monitoring.
- Client understands and accepts that default Microsoft Sentinel detection logic is applied by NCC Group as standard, and in line with the Clients' data sources. In addition to this as part of the service and with the utilisation of Azure Lighthouse the NCC Group Threat Detection Content and Logic coverage is applied in line with the MITRE ATT&CK Framework and can only be delivered based on the availability of appropriate data sources. This custom content applied using Lighthouse remains the property of NCC Group for the duration of the service agreement.
- The Client is responsible for ensuring that all data sources are forwarding log data/telemetry to their own Microsoft Sentinel instance. NCC Group is responsible for the health monitoring once data source onboarding has occurred to ensure monitoring is in place to alert on wide-scale outages across the client's estate.
- Client will ensure all network infrastructure and server infrastructure will distribute security events to the cloud based SIEM solution.
- The Client is responsible for all logging agents and syslog servers used for the collection of logging deployed within their cloud or on-premises estate.
- Client will provide any required hardware or virtual instances for the purposes of forwarding and deployment server architecture, as defined at the delivery phase.
- Provision of any required computer infrastructure to host or aggregate on Client premises (including Client cloud) collection agents.
- If API integration is required to the NCC Group ITSM portal, it is the Client's responsibility to define and pay for the work that is required to achieve this. NCC will provide guides and "how to" information (API Documentation) to the Client.
- Client agrees to inform NCC Group promptly of any changes, including network or infrastructure changes, or other circumstances that may impact the provision of the Managed XDR Service. Examples include but are not limited to:
  - Adding additional connectors or anything that materially increases the amount of data ingested into Sentinel.
  - Adding additional endpoint agents or anything that materially increases the number of alerts created with Sentinel.
  - Changes or circumstances that may impact on the service or NCC Group's ability to operate the service.
  - Any changes to systems under customer's control that may

impact on the Service or NCC Groups ability to operate the Service, for instance affecting the Lighthouse configuration connection. That may have an impact on the capacity or throughput of the service or system including changes to bandwidth and logging levels.

- Changes or circumstances that impacts the scope of the managed service and associated licenses, including additional users, monitored device or throughput.
- The Client shall be responsible for all Client specific change processes and Change Advisory Boards (CABs), relating to changes and service requests raised.)

### 2.7.1 XDR Service Boundaries

All data will be stored and processed within the clients Microsoft Azure tenancy, except in specific circumstances where data is required for further investigation, in which case this data will be stored and processed within UK.

Should the service utilisation exceed the maximum defined service ingest rate by more than 10% on a rolling monthly basis, then NCC Group shall notify the Client in writing and may charge an additional service charge for the additional utilisation.

The following section outlines features that are not in scope of the XDR Services:

- Configuring Client event sources to enable event collection.
- The calculation of running costs for the client's Sentinel instance(s)/licenses.
- The deployment of log collectors (unless otherwise specified within a Splunk managed service).
- Any involvement relating to the client's Data Protection Impact Assessments (DPIA).
- The provision of custom SOC processes, or bespoke use cases do not present within Sentinel. Except for NCC Group use case content applied with the use of Azure Lighthouse.
- SOC interactions with Client systems that are not in-scope from the Log Source Inventory [See Appendix 1 – Log Source Inventory] for forwarding events to the XDR service. This excludes other NCC Group Services that are monitored by the SOC, and do not produce logs in Sentinel.
- On-site remediation for security issues identified by the XDR Service unless a Retained Incident Response contract with NCC Group is in-place.
- Site visits, e.g., to install/cable/rack a RMA replacement
- Formal vendor training, unless explicitly defined.
- Obligation to provide a function or feature not already present or pre-identified.
- Processing of events should the defined average ingest rate exceed that agreed in this statement of work or any agreed contract change notes.
- Data retention within the Client's Microsoft Sentinel tenant is entirely configured by the Client to meet their specific retention needs and is outside of the scope of the NCC Group managed service.
- Security response automation is out of scope unless specifically agreed within this SoW

- NCC Group do not support any existing use cases (playbooks) or custom analytics (Sentinel or Defender for Endpoint rules already in place by the Client) unless these have been agreed and have been through NCC group baselining
- NCC Group is not able to provide additional Microsoft Support for Client subscriptions.
- MS Cloud App Security excludes additional MCAS configuration, event data ONLY.
- Alerting of any alarms that are not fired in Sentinel (this would include events which occur in the Microsoft ecosystem but are not deemed serious or relevant enough to fire through Sentinel).

### 2.7.2 License Prerequisites

The following overview are essential subscription components that need to be in place for NCC to deliver the service:

- Microsoft Defender for Endpoint – Plan 2
- Azure subscription and Active Directory Tenant

#### *2.7.2.1 Guidance Notes*

The following components are optional, however, NCC Group strongly advise that Clients have these components to get best value from the service:

- Microsoft Defender for Office 365 (Plan 2)
- Microsoft Defender for Identity
- Microsoft Cloud App Security
- Azure AD Premium (Plan 2)
- Microsoft Defender for Endpoint
- NCC Group can only monitor components that are fully licensed under an active Microsoft Subscription.
- It is recommended that the architecture for the set-up and configuration of Sentinel is in its own Standalone Azure Subscription. A separate Workspace is required to differentiate between log data that is retained for 90 days as standard.

- To access the Microsoft cloud services, a user must have an account associated with the Azure subscription that the service resides in. The Client can provision accounts or they can invite the NCC Group staff to join their subscription utilizing the “Cloud Admin” accounts that are provisioned to all NCC Group SOC staff.
- Some data connectors also require a license to be present in order to be enabled, these licenses are subject to changes by Microsoft and as such it is recommended you discuss with your license provider. See table below:

| Data Connector | License | Permissions |
|---|---|---|
| **Azure Activity** | None | Subscription Reader |
| **Microsoft Defender for Cloud** | Standard | Security Reader |
| **Azure Active Directory** | Any AAD license | Global Admin or Security Admin |
| **Azure Active Directory Identity Protection** | AAD Premium 2 | Global Admin or Security Admin |
| **Office 365** | None | Global Admin or Security Admin |

| | | |
|---|---|---|
| **Microsoft Defender for Cloud Apps** | MDCA | Global Admin or Security Admin |
| **Microsoft Defender for Identity** | MDI | Global Admin or Security Admin |
| **Microsoft Defender for Endpoint** | MDE | Global Admin or Security Admin |
| **Threat Intelligence Platforms** | None | Global Admin or Security Admin |
| **Security Events** | None | None |
| **Linux Syslog** | None | None |
| **DNS (preview)** | None | None |
| **Windows Firewall** | None | None |

# 3 Account Management and Governance

## 3.1 Account Management

The following section outlines the account management and governance structure for the service delivery and contract with UKHSA:

## 3.2 Account & Contract Reviews

NCC Group will have responsibility for producing the review meeting agendas and minutes with the Client having input to agenda of such meetings and shall review and/or approve minutes or add comments. As required by the Client, NCC Group's Representatives shall attend the following meetings as required by the Client:

- **Annual strategic review meetings with your designated NCC Group Account Manager** - At which the parties shall discuss the performance of this Agreement (including past and anticipated future performance, performance measures and targets, potential efficiencies and economies and the parties' strategic objectives, potential for future services & programmes and process, procedure and delivery improvement plans). These meetings shall also provide a strategic view and strategic direction and act as an executive escalation point.

- **Regular management review meetings with your designated NCC Group Account Manager** - at which the parties shall discuss the operational relationship between the parties and agree action plans in respect of the on-going scope, purpose and functioning of the relationship between the parties;

## 3.3 Technical Account Management & Service Delivery

The following service management and reporting benefits are included in the overall XDR managed service:

- Named Technical Account Manager to act as a first point of contact for operational matters and proactive management of high priority and ongoing incidents.
- Monthly reporting including, current threat intelligence picture, key metrics, analyst summary of alarms, trend analysis and executive service summary.
- Monthly calls with the named Technical Account Manager.
- Quarterly service review meeting.
- Maintained Service Roadmap to track planned service development.
- Up to 2 hours per week of additional TAM time for service improvements (e.g. workbooks/playbooks, custom detections, queries) averaged on a fair use policy over a 6 month period

## 3.4 Project Management

Each party shall nominate a project manager (each a "Project Manager") to deal with the implementation of this Statement of Work and the Services to be delivered, the Project Manager's role will be complete when the Go Live Milestones have been completed as agreed between the parties. Each party may change the identity of any of its Project Managers at any time and each Project Manager may appoint a suitable deputy or alternate to perform some or all the Project Manager's functions in their absence.

## 3.5 ITSM IT Service Management (ITSM) Integration

If API integration is required to the NCC Group ITSM (ServiceNow) portal from the Clients own ITSM it is the Client's responsibility to define and pay for the work that is required to achieve this.

- NCC will provide documented guides and "how to" information to achieve this API integration.
- NCC Group can provide a 30-minute overview of the potential API integration.
- Up to 2 hours of support from NCC Group developers to answer any questions, and to carry out any initial troubleshooting.

Additional development work, and/or support maybe available, and if so, would be chargeable at a rate that is to be defined. As an example, current integrations with Service Now have been successfully achieved. An example of where additional professional services time is chargeable for development work would be the following:

- For the development of new features, or the enhancement of functionality. Such as an enhancement to the API that would close tickets in either Service Now.
- Resolving issues/problems resulting from the Clients development of the API that cause operational impact to ITSM.

# 3.6 Escalation Process

The following escalation process would be followed in the event of a significant threat or incident.

1. Alert is received, triaged, assessed, and deemed to be a threat to the Client.
2. A ticket is raised, an L1 or L2 analyst will telephone call the escalation contact while the investigation takes place, informing them of the incident.
3. If there is any uncertainty of whether an alert is a potential threat after the assessment stage, the incident will be escalated to the Client.

# 4 Pricing of Services

## 4.1 One-off Fees

| Implementation & Setup Services | |
|---|---|
| **Commissioning of the XDR Services**<br>• One-off cost<br>• Microsoft Sentinel - SIEM Threat Detection Setup and Onboarding<br>• Design workshop<br>• Log Source inventory<br>• Includes implementation and setup, professional services and project management | **£39,850** |
| **Implementation & Setup Fees Total** | **Total – £39,850** |

## 4.2 Recurring Fees

| XDR Managed Service Fees | |
|---|---|
| **Extended Detection & Response Services**<br>• **1 Years** Service Term<br>• XDR Service – 250GB/Day Service Boundary<br>• 25,000 Endpoints covered by Defender for Endpoint<br>• Microsoft Sentinel<br>• Technical Account Management | **Year 1 – £1,059,720** |
| **Total XDR Annual Fees** | **Total – £1,059,720** |

| XDR Retained Incident Response service | |
|---|---|
| **Retained Incident Response Service**<br>• Standard Service<br>• 5 RIR Call-off days (Yr1) | **Year 1 – £25,300** |
| **Total RIR Annual Fees** | **Total – £25,300** |

| | |
|---|---|
| **Grand Total (Implementation & Setup Fees, Annual Fees and Retained Incident Response)** | **Total –** £1,124,870 |

| | |
|---|---|
| **Optional additional year 2 Annual Fees and Retained Incident Response)** | **Total –** £1,073,520 |

| | |
|---|---|
| **Optional additional year 3 Annual Fees and Retained Incident Response)** | **Total –** £1,073,520 |

## 4.3 Pricing Notes

Pricing excludes VAT and expenses. NCC Group may charge UKHSA for reasonable and properly incurred expenses in connection with the service and in line with the relevant UKHSA expense policy.

UKHSA shall inform NCC Group in writing not less than 6 months before the end of Managed Service - year 3, whether or not it wishes to extend the term of the SOW for a further period. In the event that UKHSA wishes to extend the term of the SOW, the parties will discuss in good faith any change in Fees for the extended term (and UKHSA acknowledges for these purposes that elements of the Fee are subject to agreement with third party vendors) and any reasonable amendments to the Framework Agreement, SOW or the Services that may be required.

## 4.4 Invoicing Profile

The following table outlines the breakdown of invoicing items, values and timing over the term of the Contract and Services

| Item | Value | Invoiced |
|---|---|---|
| **Implementation & Service Setup Fees + RIR Call Off Days– one off payment** | £51,350 | **upon Order Form signature** |
| **Managed Service – Year 1** | £1,073,520 | **On relevant Go Live Milestone** |
| **Total** | **£1,124,870** | |
| **Optional Managed Service – Year 2** | £1,073,520 | **The 1st anniversary of the Go Live** |
| **Optional Managed Service – Year 3** | £1,073,520 | **The 2nd anniversary of the Go Live** |

| | | |
|---|---|---|
| **Total (With optional)** | **£3,271,910** | |

## 5 Rate Card

Rate card for additional professional services engagements – other roles are available upon request.

| Role | Hourly Rate | Day Rate | Notes/Assumptions |
|---|---|---|---|
| **SIEM Consulting Day Rate** | N/A | £1,350 | Standard rate applies to all consulting days irrespective of role or seniority. |
| **Custom Analytics** | N/A | £1,350 | Standard rate applies to all consulting days irrespective of role or seniority |
| **Additional IR** | N/A | £2,200 | During standard hours. |
| **Project Management** | N/A | £1,000 | Service transition into 'Go Live'/BAU. |

***Additional services can be provided upon request and pricing provided dependant on specialism. ***

## 6 Acceptance and Agreement

UKHSA hereby confirms its acceptance of this Statement of Works.

Please sign the below signature box and return to:

| |
|---|
| *Signed:* |
| ***Name of Authorised Signatory:*** |
| ***Date:*** |

NCC Group hereby confirms its acceptance of this Statement of Works.

| | |
|---|---|
| *Signed:* | |
| ***Name of Authorised Signatory:*** | |
| ***Date:*** | |

Security Improvement Services will be delivered in accordance with the following Statement of Work:

Statement of Work – Security Improvement Services

UKHSA Security Pod

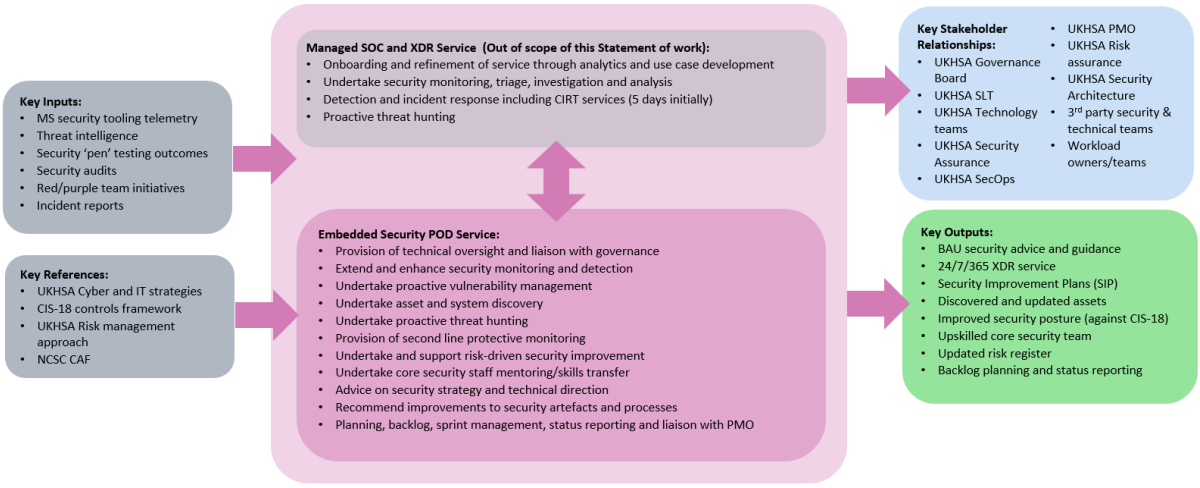
Reducing cyber risk requires comprehensive risk-based vulnerability management to identify, assess, remediate, and track all your biggest vulnerabilities across your most critical assets.

Alongside the NCC Group managed XDR solutions; will augment your cyber security posture by adding an embedded team from NCC Group – they operate as part of the client InfoSec / Security Operations team assisting in the consumption of both the managed services but also assisting the client in reacting to situational vulnerabilities. This is especially effective when considering a shared service model for example consuming the Vulnerability management data from the Microsoft implemented stack.

The POD is an embedded team (augmentation) of cyber expertise; designed to boost your internal capability within the cybersecurity areas of protection, detection, response, and recovery. This POD would utilise existing telemetry data from the estate based on existing licenses; and additional license implementation for software is outside of the scope.

This POD is designed to assist in business-as-usual activity as well as with Cyber Security Improvement capability and capacity.

The following diagram illustrates the operation of the POD; in context of the UKHSA operations.




**Embedded Security POD Service:**

This will assist you to enhance your current security posture and enhance your operations with capability and capacity to defend and monitor their network and data.

- Provision of technical oversight and liaison with governance
- Extend and enhance security monitoring and detection
- Undertake proactive vulnerability management
- Undertake asset and system discovery
- Work in parallel with the tooling, combining technical controls and security expertise to enable a collaborative decision to understand and assess your cyber exposure and take appropriate and effective actions.
- Interpretation and contextualisation of Security issues and vulnerabilities. Utilising a clear understanding and current IT strategy within the client's environment.
- Creation of prioritised planning for remediation or strategic improvement in conjunction with in-house Security and IT services.
- Visibility into software and vulnerabilities - Get a view of your software inventory, and software changes like installations, uninstalls, and patches.
- Threat analytics & event timelines - Use event timelines, and entity-level vulnerability assessments to understand and prioritise vulnerabilities.
- Tracking and managing remediation and implementation using skilled understanding of the security concerns
- Risk assess and implement some fixes; others will need to be implemented with client SME staff.
- Undertake proactive threat hunting
- Provision of second line protective monitoring
- Undertake and support risk-driven security improvement
- Undertake core security staff mentoring/skills transfer
- Advice on security strategy and technical direction
- Recommend improvements to security artefacts and processes

- Planning, backlog, sprint management, status reporting and liaison with PMO

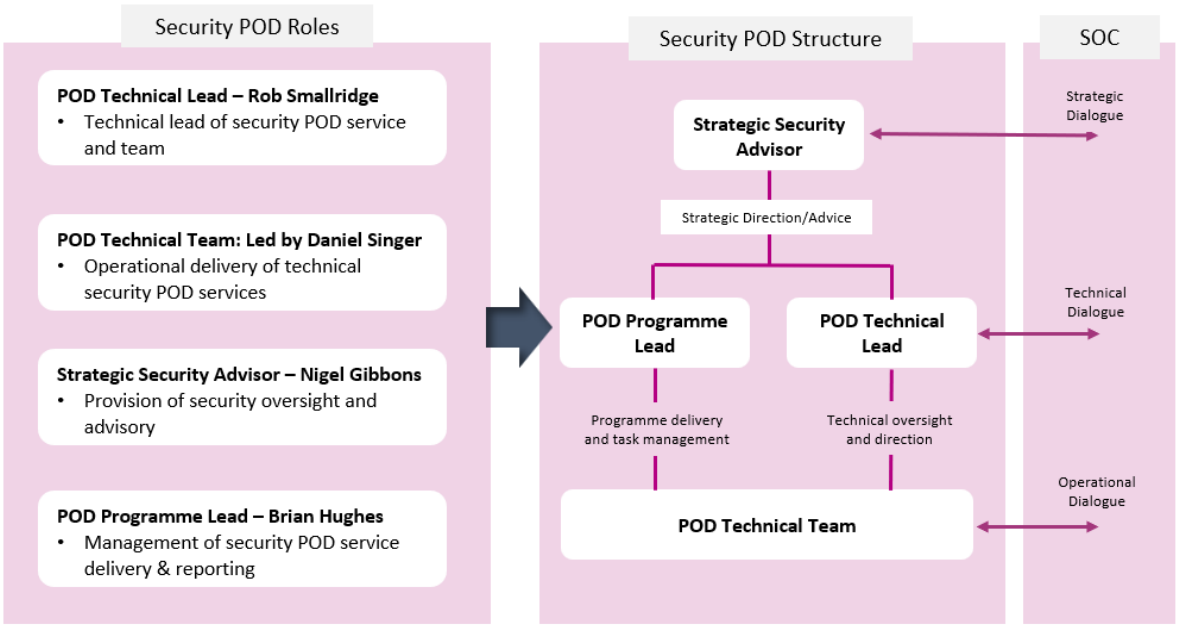
**Embedded Pod Roles and Team Structure**

The following table give examples of the roles used within an IT Security Operations team, which is expected to meet the requirement of UKSHA.

| Role | Description |
|---|---|
| **Strategic Security Advisor** | As agreed with UKHSA, key communication with C-Suite, governance, and programme management of the Security Operations POD. With Provision of security oversight and advisory. |
| **POD Programme Lead** | Management of security POD service delivery, planning and reporting<br><br>Planning, backlog, sprint management, status reporting and liaison with PMO<br><br>Security Improvement Plan creation (formal project plan) or Backlog creation and contextualisation planning. Turn current issues into executable work packages.<br><br>Contextualising with the client and creating a prioritised backlog of tasks (utilising an Agile platform or ticketing system) this is a plan/solution to help the client address the issues.<br><br>Additionally, we will:<br>• Augment with our additional inputs<br>• Prioritise for security improvement, complexity etc<br>• Agree estimates and owners<br>• Identify external dependencies (mainly inbound)<br>• Allocate Resource type |
| **POD Technical Lead**<br>**&**<br>**POD Technical Team** | Security architecture and engineering security systems working closely with various teams to conduct the following type of work<br><br>• Security Architect – improvements and design |

| | |
|---|---|
| | • AD and Azure Engineering<br>• Vulnerability Management & associated engineering<br>• Protective monitoring engineer / SIEM Engineer<br>• Network & Security Device Engineer<br>• SOC Engineer / defence second-line<br>• Blue team / Protective Monitoring<br>• Assisting in Security Improvement Fixes which are targeted at specific findings. Allowing rapid risk reduction. Enhancements as part of a rapid change program |

The interaction model and a NCC Group named individuals (already onboarded) can be seen below:




# Order Schedule 5 (Pricing Details)

1) Detailed breakdown of the charges for the MDR Services is as follows:

| Item | Value | Invoiced |
|---|---|---|
| **Implementation & Service Setup Fees + RIR Call Off Days– one off payment** | £51,350 | **upon Order Form signature** |
| **Managed Service – Year 1** | £1,073,520 | **On relevant Go Live Milestone** |
| **Total** | **£1,124,870** | |
| **Optional Managed Service – Year 2** | £1,073,520 | **The 1st anniversary of the Go Live** |
| **Optional Managed Service – Year 3** | £1,073,520 | **The 2nd anniversary of the Go Live** |
| **Total (With optional)** | **£3,271,910** | |

Security Improvement Services will be charged based on the agreed requirements in line with the rate card contained in "Order Charges" section of the Order Form. The Supplier will issue an invoice monthly in arrears. The buyer shall pay an invoice within 30 days of the date of the invoice.

# 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 |
|---|---|---|
| Managed Service Implementation Project Manager | TBC | TBC |
| Managed Service Service Delivery Manager | TBC | TBC |
| Security Improvement Delivery Lead | Rob Smallridge | |
| Security Improvement Delivery Deputy Lead | Daniel SInger | |
| | | |
| | | |

# 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 redacted 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: Short Form Security Requirements

## 3. Definitions

3.1 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:<br>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<br>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,<br>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; |

## 4. Complying with security requirements and updates to them

4.1 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.

4.2 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.

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

4.4 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.

4.5 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.

## 5. Security Standards

5.1 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.

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

5.2.1 is in accordance with the Law and this Contract;

5.2.2 as a minimum demonstrates Good Industry Practice;

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

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

5.3 The references to standards, guidance and policies contained or set out in Paragraph 5.2 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.

5.4 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.

## 6. Security Management Plan

### 6.1 Introduction

6.1.1 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.

### 6.2 Content of the Security Management Plan

6.2.1 The Security Management Plan shall:

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

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

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;

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;

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;

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

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.

6.3 **Development of the Security Management Plan**

6.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 6.4, 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.

6.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 6.3.1, or any subsequent revision to it in accordance with Paragraph 6.4, 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.

6.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 6.3.2. 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 6.2 shall be deemed to be reasonable.

6.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 6.3.2 or of any change to the Security Management Plan in accordance with Paragraph 6.4 shall not relieve the Supplier of its obligations under this Schedule.

6.4 **Amendment of the Security Management Plan**

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

emerging changes in Good Industry Practice;

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

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

any new perceived or changed security threats; and

any reasonable change in requirements requested by the Buyer.

6.4.2 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:

suggested improvements to the effectiveness of the Security Management Plan;

updates to the risk assessments; and

suggested improvements in measuring the effectiveness of controls.

6.4.3 Subject to Paragraph 6.4.4, 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 6.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

6.4.4 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.

## 7. Security breach

7.1 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.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Supplier shall:

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

minimise the extent of actual or potential harm caused by any Breach of Security;

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;

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

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.

7.3 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 – 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

Information Security Management Policy, issue date 24 April 2023, attached hereto as a separate document.

## 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 13 (Implementation Plan and Testing)

## Part A – Implementation Plan

### 1. Agreeing the Implementation Plan

1.1 The Supplier's tendered draft Implementation Plan is at Annex 1 to this Part A of Order Schedule 13. The Supplier will provide an updated, fully developed draft for Approval within 10 days of the Order Contract Start Date.

1.2 The updated draft must contain enough detail for effective management of Order Contract implementation.

1.3 The Buyer shall not unreasonably withhold Approval of the updated draft provided that the Supplier shall incorporate the Buyer's reasonable requirements in it.

### 2. Following the Implementation Plan

2.1 The Supplier shall perform its obligations in respect of Delivery and, where relevant, Testing of the Deliverables in accordance with the Approved Implementation Plan.

2.2 Changes to any Milestones, Milestone Dates, Milestone Payments or Delay Payments shall only be made via the Variation Procedure.

2.3 Where the Supplier is responsible for the failure to achieve a Milestone by the date specified in the Approved Implementation Plan this shall constitute a material Default.

### 3. Delays

3.1 If the Supplier becomes aware that there is, or is likely to be, a Delay it shall;

- Notify the Buyer in writing within 2 Working Days of becoming aware, explaining the likely impact of the Delay

- Use all reasonable endeavours to mitigate the effects of the Delay, including complying with the Buyer's reasonable instructions

## Annex 1 Draft Implementation Plan

# Part B – Testing

In this Part B to Order Schedule 13, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

| | |
|---|---|
| **"Test Period"** | the period specified in Part A to Order Schedule 13 during which Testing shall be carried out. |
| **"Test Plan"** | a plan for the Testing of the Deliverables to demonstrate compliance with Contract requirements; |
| **"Test Report"** | a test report produced by the Supplier in accordance with Paragraph 3.3 of this Part B to Order Schedule 13; |
| **"Test Success Criteria"** | the criteria specified in the Test Plan agreed pursuant to Part B of Order Schedule 13 that the relevant Deliverables must satisfy for the relevant Test to be recorded as successful. |

1 All Tests will be carried out in accordance with the Test Plan.

2 The Supplier shall submit each Deliverable for the relevant Testing no later than the date specified in the Contract for the Test Period to begin.

3 The Supplier shall submit a draft Test Plan for Approval no later than [X] days after the Start Date.

4 The Test Plan will include:

- An overview of how Testing will be carried out
- Specific details of each Test to be carried out to demonstrate that the Buyer's requirements are satisfied
- The Test Success Criteria for all Tests
- A timetable for Testing over the Test Period, this to be compliant with any Implementation Plan
- The process for recording the conduct and results of Testing
- The responsibilities of the Parties
- A categorisation scheme for test issues eg critical/serious/minor

5 The Buyer shall not unreasonably withhold Approval of the Test Plan provided that the Supplier shall implement the Buyer's reasonable requirements in the plan.

6 Unless specified in the Test Plan the Supplier shall be responsible for carrying out the Testing detailed in the plan.

7 The Buyer may require that a Buyer representative witnesses the conduct of the Tests.

8 No later than [X] days after the completion of the scheduled Test Period the Supplier shall provide the Buyer with a Test Report setting out:

- An overview of Testing carried out
- Details of each Test carried out together with the result, indicating if the success criteria were satisfied
- Details of any scheduled Tests that were not carried out
- A list of all outstanding Test issues

9 Where by the end of the scheduled Test Period the Testing process has demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer shall notify the Supplier in writing that the Testing process has been satisfactorily completed.

10 Where as a result of a Supplier default the Testing process has not by the end of the scheduled Test Period demonstrated to the Buyer's satisfaction that the Test Success Criteria have been met then the Buyer may:

- Direct the Supplier to repeat any unsuccessful Test or undertake any scheduled Test not thus far undertaken to give the Supplier an opportunity to demonstrate that the outstanding issues detailed in the Test Report have been resolved; or

- Notify the Supplier that testing has been satisfactorily completed subject to rectification of outstanding issues within a period specified by the Buyer. Failure to rectify the relevant issues within the period specified shall be a material Default; or

- to reject the relevant Deliverables and to invoke Clause 3.2.12; or

- to reject the relevant Deliverables treating this as a material default and invoking the Buyer's termination right under Clause 10.4.1

# Order Schedule 14 (Service Levels)

The Service Levels applicable to the MDR Services are set out in (i) the Statement of Work for MDR Services contained within Order Schedule 4 (Order Tender and (iI) sections 10.1, 10.7, 10.8 and 10.9 of the Supplier's MDR Master Service Description and SLA Document attached hereto as a separate document. In the event of any conflict between the terms of this Statement of Work and the MDR Master Service Description and SLA document, the terms in the Statement of Work shall govern.

Service Levels are not applicable to Security Improvement Services.

# Order Schedule 15 (Order Contract Management)

## 1. DEFINITIONS

**2.** 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 4 of this Schedule; |

## 3. PROJECT MANAGEMENT

4. 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.

5. 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.

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

## 7. ROLE OF THE SUPPLIER CONTRACT MANAGER

7.1 The Supplier's Contract Manager shall be:

**8. 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;**

**9. 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;**

**10. able to cancel any delegation and recommence the position himself; and**

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

11.1 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.

11.2 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.

## 12. CONTRACT RISK MANAGEMENT

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

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

**13. the identification and management of risks;**

13.1.1 the identification and management of issues; and

13.1.2 monitoring and controlling project plans.

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

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

**9.**

## 14. Role of the Operational Board

15. 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.

16. 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.

17. 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.

18. 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.

19. 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:

**Guidance note**: Details of additional boards to be inserted.