Order Schedule 4 (Order Tender)

1 TERM

Initial Term:	[redacted]

2 SERVICES AND CHARGES

Description	Charges
Incident Response – Annual retainer • 100 analyst hours IR Call-off Budget per Contract Year • Services as described in attached Services Schedule	[redacted]
Incident Response – Top-up hours • Available to be added to the retained hours – in 50 hour bundles	[redacted]

[redacted]

3 SPECIAL TERMS

The Buyer acknowledges that that the Supplier Services are provided under the UK National Cyber Security Centre's (NCSC) certified Cyber Incident Response (CIR) scheme and agree that, under the terms of that scheme, The Supplier may be required to share a copy of the Post-Incident Reports with NCSC on a confidential basis. The Supplier shall consult with the Buyer before such disclosure to NCSC and, to the extent permitted by the terms of the CIR scheme, co-operate with the Buyer in minimising the disclosure to the extent reasonably practicable (for example, by redacting sections of the reports).

INCIDENT RESPONSE (IR) RETAINER – SERVICES SCHEDULE

1 DEFINITIONS

1.1 The following definitions apply in this Schedule:

IR Call-off Budget: the fixed capacity set of incident response analyst hours included with the Services for each Contract Year as specified on the Order, together with any additional 'top-up' hours purchased pursuant to a Change Request.

IR Hotline: the meaning given in section 6 (Incident Response) below.

Initial Buyer Call: the meaning given in section 6 (Incident Response) below.

Specialist Call Back: the meaning given in section 6 (Incident Response) below.

Task: each engagement for a set of incident response or incident readiness activities to be undertaken by the Supplier, as mutually agreed in writing in accordance with this Schedule.

Working Day: a day other than a weekend or public/federal holiday (and, in the case of the USA, the day after Thanksgiving) in the location/time-zone specified on the Order (or the location from which the Supplier provides the Services, if not specified).

Working Hours: an 8 hour work period between the hours of 0830-1730 on Working Days.

1.2 Any communications 'in writing' under this Schedule may be by email.

2 SERVICE OVERVIEW

2.1 The Supplier's Incident Response Services provide access to specialist IR analysts from the Supplier's cyber security incident response team to support the Buyer with the response to cyber security incidents 24x7x365, and to assist the Buyer with incident readiness activities.

2.2 The Services provide an IR Call-off Budget which the Buyer can call-off in accordance with this Schedule, with the option to purchase 'top-ups' to the IR Call-off Budget as required.

3 ON-BOARDING

3.1 To set up the Services, the Supplier shall review any key documentation provided by the Buyer and hold an on-boarding workshop with the Buyer to complete the following on-boarding activities:

(a) gain an understanding of the Buyer's IT estate, security controls, and detection and response capability;

(b) discuss the Buyer's internal business processes for security incident response and agree how these will integrate with The Supplier cyber security incident response team;

(c) agree the key points of contacts regarding the Services;

(d) confirm the involvement of any third parties (e.g. The Buyer's IT suppliers) and agree the roles and responsibilities regarding communication with and management of those third parties in respect of security incident response; and

(e) review any previous incidents and known vulnerabilities affecting the Buyer's IT estate.

3.2 The workshop shall be held at a time and location to be mutually agreed, which may be by teleconference.

3.3 The Supplier shall also work with the Buyer to establish a secure email channel for the purposes of communications regarding the Services.

3.4 Upon request from the Buyer, The Supplier shall provide a short report (Deliverable DEL-IR-01) based on the information gathered through the on-boarding activities setting out any key observations and recommendations as to how the Buyer could improve its incident response capabilities.

4 SCOPE OF THE SERVICES

4.1 Following completion of on-boarding, the Supplier shall provide the Buyer with access to specialist analysts from its cyber security incident response team on an ad-hoc basis during the Term for incident response Tasks, including:

(a) **Evidence Acquisition:** Acquisition of forensic images from a range of devices;

(b) **Disk Image Analysis:** Review of a disk image to identify evidence of malicious activity including presence of remote access tools;

(c) **Attack Attribution:** Help to identify the actors responsible for the attack;

(d) **Emergency Monitoring:** Deployment of host-based software to collect rich data for monitoring in support of an investigation;

(e) **Memory Forensics:** Capture and review of memory to identify malicious processes or find decrypted command and control messages;

(f) **Network Capture Analysis:** Review of packet capture files to extract and analyse content of suspicious network sessions;

(g) **Remediation Advice:** Help with identifying appropriate remediation actions, scheduling the implementation and confirming success;

(h) **Log Data Analysis:** Review of log files including proxy, VPN, and IDS appliances as well as Windows Events and other host-based logs;

(i) **Malware Analysis:** High-level malware analysis to extract key signatures and behaviours;

(j) **Reverse Engineering:** Full reverse engineering of malware samples to try and recover encryption routines and capability;

(k) **Third Party Enquiries:** Help with requesting support or responding to requests from external bodies;

(l) **Email Analysis:** Review of a suspected email to determine if the content is safe, or bulk analyses to identify if email was the attack vector;

(m) **Forensic Data Recovery:** Forensic extraction or retrieval of data;

(n) **Mobile Device Forensics:** Recovery and analysis of data from a mobile device;

(o) **Forensic Investigation:** Investigate a cyber security incident end to end;

(p) **Threat Hunting:** Proactively searching through networks and systems to detect and isolate advanced threats that evade existing security solutions;

(q) **Endpoint Detection and Response (EDR):** Using EDR software on client infrastructure in response to a cyber incident;

(r) **Cloud Incident Response / Forensics:** Forensics and incident response on multiple cloud platforms;

(s) **Post Incident Monitoring:** Monitoring using EDR tools after a cyber attack;

(t) **Executive Incident Support:** Emergency non-technical consulting support to the organisation's management or executive teams during a cyber incident; or

(u) **Technical Incident Management:** Assistance in orchestrating and undertaking the technical aspects of wider incident response activities.

4.2 The specific incident response Tasks to be conducted are subject to mutual agreement in writing in accordance with section 6 (Incident Response) below.

4.3 The Services may also be used for incident readiness Tasks where mutually agreed in accordance with section 7 (Incident Readiness) below.

4.4 The Supplier shall be under no obligation to provide the Services until on-boarding has been completed (but may do so at its discretion if requested by the Buyer).

5 IR CALL-OFF BUDGET

5.1 The Services are provided on a fixed capacity basis up to the total IR Call-off Budget that has been purchased by the Buyer. The Services provide the Buyer with an inclusive IR Call-off Budget as specified on the Order for each Contract Year. The Buyer has the option to purchase additional IR analyst hours to 'top-up' the IR Call-off Budget via a Change Request. For more extensive engagements, the Buyer may place a separate order for consultancy services.

5.2 Any budget/effort estimates provided to the Buyer are indicative estimates only. The draw down from the IR Call-off Budget will be calculated based on the actual hours worked on the agreed Tasks using:

(a) minimum units of one hour for any incident response Tasks; and

(b) minimum units of four hours for any incident readiness Tasks.

5.3 The Supplier will be under no obligation to commence, or continue (for in-progress Tasks), providing the Services (including the completion of any agreed Deliverables) in the event that the IR Call-off Budget is exhausted. The Supplier recommends that the Buyer maintains a balance of at least 40 analyst hours in the IR Call-Off Budget to prevent any delays in responding to new incidents.

5.4 The inclusive IR Call-Off Budget specified on the Order is provided for each Contract Year and is valid only for that Contract Year. Any inclusive IR Call-off Budget that is unused at the end of the Contract Year is non-refundable and may not be carried over to subsequent Contract Years. IR Call-off Budget may not be brought forward from future Contract Years.

5.5 Any 'top-ups' to the IR Call-Off Budget purchased pursuant to a Change Request are valid for 12 months from the date of the Change Request or until the end of the Term (whichever is the sooner), and are non-refundable if not used.

6 INCIDENT RESPONSE

6.1 The Supplier shall maintain a 24x7x365 telephone hotline for the Buyer to report incidents (the "**IR Hotline**"). When the Buyer believes a security incident has occurred and wishes to engage the Services, the Buyer shall call the IR Hotline (the "**Initial The Buyer Call**"). The Initial Buyer Call will be answered by an operator from one of The Supplier' global delivery centres who will capture initial details about the security incident and provide an estimate on the timing of the Specialist Call Back.

6.2 Following the Initial Buyer Call, an IR analyst will call back the Buyer (the "**Specialist Call Back**") to discuss the incident in more detail and agree the details of the Task that the Supplier will undertake to assist with the response, including whether any on-site support is required.

6.3 Following the Specialist Call Back, the Supplier shall then summarise the details of the agreed Task in writing, incorporating an initial indicative estimate of the IR Call-off Budget required. The Buyer shall then respond in writing to confirm whether or not to proceed.

6.4 Following written confirmation from the Buyer, The Supplier shall proceed with the agreed Task. Where the Buyer has requested an 'emergency' response the SLA-IR-01 (Emergency Response) Service Level (as set out in section 12 (Service Levels) below) will apply. The Supplier shall use reasonable endeavours to meet any timescales agreed with the Buyer in writing for the performance of the Task.

6.5 Throughout the Task, The Supplier shall keep the Buyer updated on progress and the Buyer's usage of the IR Call-off Budget. Any changes/extensions to the scope of the agreed Tasks will be subject to mutual agreement in writing.

6.6 Where requested by the Buyer, upon completion of each Task the Supplier shall prepare a short report (Deliverable DEL-IR-02) summarising the incident response actions taken and any analysis outputs, together with any observations and recommendations. The effort to prepare this report will be drawn from the IR Call-off Budget.

7 INCIDENT READINESS

7.1 Provided that the Buyer has purchased an inclusive IR Call-off Budget (excluding any 'top-ups') of at least 100 analyst hours per Contract Year, the Buyer may, subject to the other provisions of this section 7 (Incident Readiness), use the IR Call-off Budget for incident readiness activities, including:

(a) **Incident Response Training:** CPD accredited incident response training for information security teams;

(b) **Incident Response Readiness Assessment:** Readiness assessment of all aspects of the organisation's incident response capability;

(c) **Incident Response Tabletop Exercise - Technical**: Interactive bespoke exercises designed to test the organisation's technical team's response to a cyber attack;

(d) **Incident Response Tabletop Exercise - Board:** Interactive bespoke exercises designed to test the organisation's board / executive management response to a cyber attack;

(e) **Incident Response Process / Playbook Creation:** Customised incident response process and playbooks created by our security experts using learnings from real life incident response experience;

(f) **Incident Response Process / Playbook Review:** Review of existing incident response process and playbooks by The Supplier' consultants using learnings from real life incident response experience;

(g) **Post Incident Review:** Review of a cyber incident and the response to it; or

(h) **Purple Team Workshop:** Independent review of the Buyer's incident response team's response to a red team penetration test / exercise

7.2 Such incident readiness activities must be scheduled with the Supplier agreement at a mutually convenient time, and subject to resource availability. The Buyer should raise a request with the Supplier with as much notice as possible, and acknowledges that The Supplier typically requires a minimum of 4-6 weeks' notice. The scope and timescales of any incident readiness Tasks will be subject to mutual agreement in writing.

7.3 The Supplier may decline requests for incident readiness activities that would deplete the IR Call-Off Budget below the minimum recommended balance required to respond effectively to new incidents.

8 CANCELLATION OF AGREED TASKS

8.1 The Buyer may cancel a Task at any time upon immediate written instruction to The Supplier, provided that:

(a) the Buyer shall give as much notice as reasonably possible of any cancellation;

(b) all Services performed up to and including the time of such cancellation (and any travel time to return from The Buyer site) will be chargeable and drawn from the IR Call-off Budget;

(c) the Buyer shall pay any expenses or material costs incurred or committed in respect of the cancelled Tasks which, in the Supplier' reasonable opinion, cannot be defrayed elsewhere; and

(d) for incident readiness Tasks, 16 hours will be deducted from the balance of the IR Call-Off Budget if the Buyer cancels a Task less than 10 Working Days prior to its scheduled start date (or once a Task has already started).

8.2 Any requests to reschedule a Task are first treated as a cancellation in accordance with the above. Scheduling a replacement Task is then subject to mutual agreement in writing.

8.3 For the avoidance of doubt, cancellation of an agreed Task shall not terminate the Order Form.

9 WORKING HOURS AND LOCATION

9.1 The Incident Response Services described in Section 6 (Incident Response) are provided 24x7x365. The Specialist Call Back and initial activities for incident response Tasks will always be performed remotely from one of the Supplier' global delivery centres. Subsequent support may be provided on-site where mutually agreed in writing (and subject to availability). Where the Supplier agrees to provide on-site incident response, the travel time will be chargeable and drawn down from the IR Call-off Budget.

9.2 All incident readiness Tasks are provided during Working Hours only. The location of the incident readiness Tasks will be subject to mutual agreement in writing.

9.3 All travel and subsistence expenses for any on-site work, and any materials expenses, will be charged in addition to the Charges in accordance with the Order Form section Reimbursable Expenses.

10 TOOLING

10.1 In support of an agreed Task, The Supplier may recommend that the Buyer deploys certain hardware or software to the Buyer network for a limited period. Where the use of such hardware or software would incur additional Charges, this shall be subject to mutual agreement pursuant to a Change Request.

10.2 Such hardware and/or software is made available to the Buyer:

(a) subject to the Buyer's compliance with any additional Buyer responsibilities (for example regarding support to installation) and licence terms as may be set out or referenced in any accompanying documentation;

(b) for the Buyer's internal use only in relation to, and for the duration of, the agreed Task; and

(c) on an 'as-is' basis and the Buyer acknowledges that The Supplier does not make any warranty or representation in relation to such hardware or software or any results they may produce.

10.3 The Buyer shall uninstall and return all such hardware and software to The Supplier within 30 days of completion of the applicable Task, unless it is otherwise agreed in writing to keep such hardware or software installed for a longer period in readiness for potential use on future Tasks.

10.4 Where The Supplier agrees that the Buyer may securely destroy (rather than return) any hardware, for example for security reasons, the Buyer shall reimburse the Supplier for the cost of a replacement.

11 REVIEW MEETINGS

11.1 The Supplier shall organise quarterly service review teleconference calls with the Buyer ("**Quarterly Service Reviews**"). The purpose of the Quarterly Service Review is to review any incidents that have occurred during the quarter, discuss any trends or views on the Buyer's incident response capabilities, discuss potential incident readiness Tasks and review the Buyer's usage of the IR Call-off Budget.

11.2 Where the Term is longer than 12 months, The Supplier shall organise annual review meetings ("**Operational Review**") with the Buyer at the start of Contract Year 2 and at the start of each Contract Year thereafter until the end of the Term.

11.3 The purpose of the Operational Review is to review and update the details agreed during the initial on-boarding workshop to ensure they are still valid and incorporate any 'lessons learned' identified from security incidents that may have occurred during the previous Contract Year.

11.4 The Operational Reviews shall be held at a time and location to be mutually agreed, which may be by teleconference. Following each Operational Review, The Supplier shall, if requested by the Buyer, update the details of the on-boarding report (Deliverable DEL-IR-01).

12 SERVICE LEVELS

12.1 The following Service Level will apply to any incident response Tasks:

Ref	Name	Measure	Service Level
SLA-IR-01	Emergency Response	Time elapsed from the end of the Initial The Buyer Call to the Specialist Call Back. This Service Level only applies where the Buyer requested an 'emergency response' in the Initial The Buyer Call.	2 hours
SLA-IR-02	Emergency Response IR Hotline	Time elapsed from the placement of the Initial Buyer Call to the answer from the IR Hotline.	15 minutes
SLA-IR-03	Emergency Response Resources on site	Time elapsed from Buyer request. The Supplier will use reasonable endeavours to meet the Service Level and any service credit will be at the Supplier's discretion.	24 hours
SLA-IR-04	Emergency Response Additional specialist support	Time elapsed from Buyer request. The Supplier will use reasonable endeavours to meet the Service Level and any service credit will be at the Supplier's discretion.	72 hours

12.2 The Service Level only applies following completion of the on-boarding activities and where the Buyer has sufficient IR Call-off Budget available. The Service Level does not apply to incident readiness Tasks.

12.3 The Service Level will be extended during any period where The Supplier is waiting for access to materials, information, premises, records, systems, personnel or other assistance or authorisation from the Buyer or any third parties, in particular but without limitation where The Supplier is awaiting written confirmation to proceed from the Buyer following the Specialist Call Back.

12.4 In the event that The Supplier fails to meet the Service Level of SLA-IR-01 and SLA-IR-02 in respect of an individual incident response Task, the Buyer shall be entitled to receive a single service credit of 16 hours which shall be added to the IR Call-off Budget for that Contract Year, subject to an aggregate cap of 64 hours in each Contract Year. The entitlement to such service credits shall represent the Buyer's sole remedy for the failure by The Supplier to achieve the Service Level.

13 DELIVERABLES

13.1 The Supplier shall provide the following Deliverables as the output of the Services:

Ref	Deliverable	Description	Timing
DEL-IR-01	On boarding report	Short report setting out any key observations and recommendations made by The Supplier during the on-boarding activities as to how the Buyer could improve its incident response capabilities. This is provided only if the Buyer has requested an on boarding report. Where requested by the Buyer, The Supplier will update this report following each Operational Review.	Within 10 Working Days of the completion of the on-boarding activities or the annual Operational Review.
DEL-IR-02	Post-Incident report	Short report setting out the incident response actions taken, including the output of any analysis activities, together with any observations/recommendations. This is provided only if the Buyer has requested a post-incident report.	Within 10 Working Days of the completion of each incident response Task

13.2 The Buyer may request additional or interim Deliverables in respect of each incident response Task, subject to agreement by The Supplier in writing. The Supplier will use reasonable endeavours to meet any reasonable timescales requested by the Buyer for these additional/interim Deliverables.

13.3 Specific Deliverables may also be mutually agreed for any incident readiness Tasks.

13.4 All Deliverables are deemed accepted on delivery. Any amendments requested by the Buyer are subject to agreement by The Supplier and the effort will be drawn from the IR Call-off Budget.

14 DEPENDENCIES

14.1 The Buyer shall be responsible for meeting the following dependencies:

Ref	Dependency	Description	Required by
DEP-IR-01	Secure email channel	The Buyer shall provide a secure email channel for communications regarding the Services (using one of The Supplier' supported formats). The Supplier is only responsible for configuring The Supplier' own mail servers for the agreed secure email channel; the Buyer is responsible for correctly configuring its own equipment.	Completion of on-boarding
DEP-IR-02	Documentation	The Buyer shall provide The Supplier with any relevant documentation regarding the Buyer's network architecture, incident response management capabilities/processes and details of past incidents and known vulnerabilities.	Prior to the on-boarding workshop, with regular updates through the Term
DEP-IR-03	Meeting attendance	The Buyer shall ensure the attendance of the relevant The Buyer personnel at the on-boarding workshop and any review meetings.	For each scheduled meeting/workshop

Ref	Dependency	Description	Required by
DEP-IR-04	Engagement process	The Buyer shall raise all requests for Services in accordance with sections 6 (Incident Response) and 7 (Incident Readiness) and provide prompt confirmation in writing of the Task details submitted by The Supplier.	As required
DEP-IR-05	End user interaction	The Buyer shall be responsible for all contact with its end-user community regarding any security incidents. The Supplier shall not be obliged to have any direct contact with end users.	Throughout

15 AFFILIATE USE

15.1 The Buyer may use the Services for Tasks with Buyer Affiliates provided that the Services are always managed via the Buyer, including that:

(a) all Tasks are managed through, and all Deliverables are delivered to, the same Buyer point of contact;

(b) there is a single, common set of business processes for incident response, agreed through a single on-boarding workshop and annual Operational Review;

(c) the Quarterly Review Meetings and Operational Reviews will be held with the Buyer only.

If any Affiliates request a direct engagement with The Supplier this would require a separate Order Form.

16 ADDITIONAL TERMS

16.1 As a result of providing the Services, the Supplier may derive information, data and know-how relating to threat actor identities and methodologies, samples of malware, indicators of compromise (including suspect domains, IP addresses, URL patterns seen in an attack, compromised websites and email addresses used by threat actors, malware hashes, file paths, and registry keys) and other intelligence regarding cyber security threats. Such threat intelligence information, data and know-how does not constitute Buyer Data. The Supplier may use this threat intelligence in providing cyber security services to other the Buyers and in sharing anonymised threat intelligence with government agencies and industry bodies. In turn, the Supplier may use the threat intelligence it has gained from its other the Buyers and government and industry partnerships in providing the Services to the Buyer. Where The Supplier shares details of any threat intelligence it has received from third parties with the Buyer, the Supplier will do so in good faith and make reasonable attempts to verify accuracy however the Supplier provides no warranty with regards to the accuracy or completeness of such threat intelligence and the Buyer's reliance on it is at its own risk, to the fullest extent permitted by applicable law.

16.2 In response to a security incident, the Supplier may recommend that the Buyer authorises the Supplier to notify a relevant government agency or industry body with detailed information relating to the incident that may identify the Buyer. The Supplier will only recommend sharing such information where strictly necessary and where in doing so The Supplier believes it will enable The Supplier to provide the Services to the Buyer more effectively. The Supplier will only share such detailed information that identifies the Buyer with the Buyer's prior written consent (email communication is acceptable), unless otherwise required by law.