SCHEDULE J: SERVICE DEFINITION FOR CYBER SECURITY OPERATIONS CENTRE SERVICES

1. Service Description for Cyber Security Operations Centre Services

Exponential-e Cyber Security Operations Centre Services comprise of the Services in the packages detailed in section 3 below (and as specified on the Order Form) and will be provided by Exponential-e from its Cyber Security Operations Centre (CSOC). To accommodate each customer's IT environment, a Statement of Work (SOW) will support each engagement. The SOW contains the timescales for deliverables (such as reports or system outputs and analysis), any target service level for monitoring the Services, and the web reporting portals to be used. Once signed by both Parties, the SOW is deemed to form part of the Contract. The definition of Contract in the General Terms shall therefore be considered amended accordingly. In the provision of all CSOC Services, Exponential-e acts as a consultant providing advice to the Partner/End User in relation to the security of its estate. Exponential-e will not be liable for any failure to meet any target service levels where such failure arises as a direct or indirect result of changes, which the Partner/End User may implement. Changes made by the Partner/End User are made at the Partner's/End User's sole risk. It is the Partner's / End User's responsibility to qualify the impact of any potential change and to satisfy itself that the change is required, actionable and supportable for the security of its estate.

2. On boarding and Engagement

A CSOC engineer will collect all the relevant information to create the SOW. Once the Partner has accepted the SOW then the provision of the Unified Security Manager device ("USM") (a deployed VM server loaded with a software device) and its connectivity will begin and be considered complete when the USM receives its first log. The Service Commencement Date is deemed to have occurred in relation to the CSOC Service once the first log is ingested/collected by the USM. During the on boarding stage, the Parties will identify devices that are: (a) within the Partner's / End User's estate; and (b) within scope. Exponential-e will provide the Partner/End User with access to a software agent to enable the servers to report log information to the USM. Devices such as firewalls that generate syslog will not require the agent. The log/syslog information will also be aggregated, correlated and processed by the USM device. Exponential-e will also set out in the SOW the agreed list of activities for each Party for the "flags" that are detected. The Partner / End User will be provided with credentials to have a "read only" view of the USM device. In the event that following on boarding there is a "flag", CSOC will respond to the Partner/End User as agreed in the SOW subject always to the severity of the incident monitored. The Parties will also discuss on a weekly basis at a time agreed between the Parties, the output logs and the variations which occur in the logs. CSOC will refine and tune these output logs throughout the on boarding stage. Throughout the engagement, the outcome of the initial scan report will be discussed with the Partner / End User so that the Partner / End User has the opportunity to ask questions in relation to that report. If any remedial actions are advised, it is the Partner's / End User's responsibility to propose (working with the CSOC) how it wishes to remediate the issues. During the course of the engagement and at a time agreed with the Partner and on no more than quarterly basis, a CSOC engineer will have a telephone discussion with the technical contact of the Partner to discuss the technical operation of the Service. If during the engagement, a monitored asset which forms part of another service which Exponential-e is providing to the Partner has a fault, CSOC will notify the Partner and the relevant Exponential-e support team who will then liaise with the Partner as set out in the applicable Service Document for the affected Exponential-e service.

3. The Cyber Security Operations Centre Services Packages

(a) Security Incident and Event Monitoring (SIEM)

To enable these CSOC Services a SIEM will be deployed by Exponential. The SIEM consists of a USM device. This USM device will collect log information from the Partner's / End User's monitored asset. This provides a view via a web-based portal of the whole of the Partner's / End user's estate within scope of the SOW. The Partner / End User will need to provide a rack environment for the USM at its Site.

(b) Threat Detection

Exponential-e will alert and monitor the Partner's / End User's estate to seek out existing un-triggered threats or vectors for attack that could be monopolised. This is a service consisting of a deployed USM device and the proactive monitoring and testing of the Partner's End User's estate on a 24x7x365 basis. The result of the monitoring consists of a web-accessed dashboard with a report on the testing schedule, which is highlighted on a red, amber and green (RAG) priority basis.

CSOC will assist the Partner/End User in establishing the remedial action to take in all cases.

(c) Internal Vulnerability Monitoring

Exponential-e will monitor the Partner's/End User's estate in order to seek out vulnerabilities and to implement relevant remedial actions. This Service consists of a deployed USM device and the proactive monitoring and testing of the Partner's/End User's estate on a 24x7x365 basis. The result of the monitoring and testing consists of a web-accessed dashboard with a report on the testing schedule, which is highlighted on a red, amber and green (RAG) priority basis.

CSOC will assist the Partner / End User in establishing the remediation action to take in all cases.

(d) Monitored Compliance

This offers a managed platform that monitors the status of the Partner's / End User's estate compliance based on the Partner's / End User's elected compliance standard controls and any detected events and threats on a 24x7 x365 basis. The alert will notify the Partner/End User of industry best practice to follow in order to maintain the security of their estate to their elected compliance standard. The Partner/End User will also be notified as part of this package of actions how to protect against the particular threat or incident that has been detected.

Exponential will use its reasonable endeavours to provide the Partner with a monthly report and a supporting call in order to explain any technical issues in greater detail. The Partner will also be supplied with credentials to enable the Partner to log in to a web-based portal in order to obtain further information on the status of its estate compliance.

4. CSOC Service Demarcation Point (SDP)

The Partner / End User will be responsible for the hosting of a USM device at its Site(s) or datacentre space and the required network configuration to ensure that the USM can communicate with the managed platform.

The SDP is the supplied USM device. This will be the point up to which Exponential-e has responsibility.

5. Change Management

A total of 10 changes per month shall be provided at no additional charge. Additional changes shall be subject to additional charges. It is possible that a single change request may include multiple changes, in which case each change will be count as a single change. Changes requested will normally involve a change to priority notification or change to monitored device and will normally only be carried out during Normal Business Hours. Exponential-e cannot be held responsible for lack of reporting or security information in implementing requested changes but all change requests are checked to attempt to ensure that issues will not occur. Change request target lead times are as follows: High Priority Request – 4 hours, Normal Priority Request – 8 hours*

*as determined by Exponential-e acting reasonably.

6. Access and Reporting

The USM enables the Partner / End user to have visibility of its assets which are in scope and which are monitored assets. These will be visible via a web portal that the Partner / End User can access. The Partner / End User will have access to real time information on how the devices are operating and can download reports.

7. Target Service Commencement Date

The Target Service Commencement Date will be set out in the SOW and shall be calculated from order acceptance. The Partner accepts that where Exponential-e agrees to delay the Service Commencement Date following the Partner's written request, or the Target Service Commencement Date is not met as a result of the Partner's / End User's delay or failure to fulfil its obligations in respect of this Service or under the Contract, the Annual Charges for that Service shall be payable by the Partner from the Target Service Commencement Date

set out in the SOW, unless otherwise agreed in writing between the Parties. Nothing in this clause shall oblige Exponential-e to agree to any delayed handover of this Service.

8. Service Level Agreement

For incidents logged to the CSOC by the Partner, the priority can be set by the Partner acting reasonably, when logging the incident, via either email or telephone.

Severity Level	Description
S1	A critical business service is non-operational impacting the customer organisation, multiple users or multiple sites; or severe functional error or degradation of service affecting production, demanding immediate attention. Business risk is high, with immediate financial, legal or reputational impact.
S2	The customer is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the customer or service has been affected, although a workaround may exist; or application functionality is lost; or significant number of users or major site is affected. Business risk is high.
S3	The customer is experiencing a problem that causes moderate business impact. The impact is limited to a user or a small site; or incident has moderate, not widespread impact; or the customer or IT service may not have been affected. Business risk is low.
S4	Standard service request (e.g. User Guidance); or updating documentation. Low or Minor localised impact.

Target Availability

Service	Target Availability
Cyber Security Operations Centre Services - Portal	99.9%

Service Credits

		Service Credit*
Measure	>0.1 below Target	10%

The Service Credit is applied as a percentage of the Monthly Charge for the CSOC Service where the portal is not available.