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 comprises all of the Service packages detailed in section 3 below and will be provided by Exponential-e from its Cyber Security Operations Centre (CSOC).

The Order Form will set out (i) the number of USM virtual sensors to be deployed (ii) the number of days' worth of log the Cloud Unified Security Manager system ("USM System") will collect, store (subject to contracted capacity) and accordingly how many days of log the Partner is able to view at any given time and (iii) the maximum storage capacity for the USM System. The options for (ii) above available are:

- **Essentials Option:** 15 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing.
- **Standard Option:** 30 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing.
- **Premium Option:** 90 days of logs will be collected and stored (subject to contracted capacity) by the USM System for viewing.

It is the Partner's/End User's responsibility to determine which of the options above and what maximum storage capacity it requires taking into account its IT environment including any requirements mandated by its Compliance department. Exponential-e will assist the Partner in deciding which option to select and an appropriate maximum storage capacity but this is conditional on the Partner acknowledging and accepting that Exponential-e used information provided by the Partner during due diligence as the basis for calculating the amount of storage required for the Partner's/End User's USM System. This included data such as the amount of assets which require monitoring, the number of users and possible applications being used by such users (example EDR's, Office365 accounts, InTunes MDM's etc).

Exponential-e makes use of known averages per asset type and user activity. The Partner therefore accepts that any less "mature" environment in terms of application configuration, user abuse or external nefarious activity (DDoS for example) may cause the initial scoping storage requirements to require review and an upgrade.

Notwithstanding that the Partner has pre-selected an option and maximum storage capacity on the Order Form, it is possible for the Partner/End User to exceed the storage limit of that pre-selected option for the following non-exhaustive reasons: misconfiguration, where there is an introduction of non-scoped equipment and/or influx of new users to the environment. In the event that storage limit is exceeded, it may result in the following:

a. The system not storing event data. Event data will not be stored until the beginning of next chosen option (15 days, month or quarter). At the Partner's request, Exponential-e may filter some of the additional log sources. However, by doing so, the Partner/End User accepts that this may result in the loss of visibility over its relevant data.

b. The USM System no longer storing events in the searchable data store, but it will continue to generate alarms, run authenticated asset scans and store raw logs associated with events in cold storage (logs collected and stored in the last 365 days). However, by not having immediately searchable and available logs under the stored events menu, the Partner may be in breach of its own or any other Compliance rules it is required to adhere to. The Partner accepts responsibility for any such breach.

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 in relation to the security of the End User's 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.

On boarding and Engagement

Exponential-e will collect all the relevant information to create the SoW. Once the Partner has accepted the SoW, the provision of the USM System and the deployment of the scoped USM virtual sensor(s) will begin and be considered complete when the USM System receives its first log. The number of USM virtual sensor(s) deployed in respect of a Partner/End User will depend on the number of assets to be monitored and the quantity of zones (i.e. whether the Partner's servers are located in more than one location namely; Azure, AWS and at data centres). Additional Charges apply in respect of each additional USM virtual senor to be deployed.

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 System. A NXLog collection tool will need to be deployed on any Microsoft server in order to enable logging and monitoring by the SIEM by the Partner unless Exponential-e is managing that Microsoft server as part of a Flex Manage Service. Devices such as firewalls that generate syslog as well as other solutions that might provide an API integration will not require the agent. The log/syslog information will also be aggregated, correlated and processed by the USM System. 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 will be provided with credentials to have a "read only" view of the USM System. In the event that following on boarding there is a "flag", CSOC will respond to the Partner as agreed in the SoW subject always to the severity of the incident monitored. The Parties will also discuss on a weekly basis during the on-boarding stage, 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 so that the Partner has the opportunity to ask questions in relation to that report. If any remedial actions are advised, it is the Partner'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.

The Cyber Security Operations Centre Services Packages

(a) **Security Incident and Event Monitoring (SIEM)**

The SIEM consists of at least one USM virtual sensor. This USM virtual sensor will collect log information from the Partner's/End User's monitored assets. This provides a view via a web-based portal of the whole of the Partner's estate within scope of the SoW. The USM virtual sensor can be deployed in public cloud environment, private cloud or using a physical server.

For public cloud deployments, the Partner shall be responsible for the installation of the SIEM in their instance.

For private cloud deployments, the responsibility for the installation shall be on the entity responsible for management of the cloud platform.

For physical server deployments, Exponential-e will provide a pre-configured server, the responsibility for plugging and providing connectivity to such server will be the Partner's responsibility (and/or any 3rd party employed by the Partner/End User to manage its infrastructure).

The Partner acknowledges and accepts that any failure: (a) on its part to install the SIEM (b) on the part of the entity responsible for managing the private cloud deployment to install the SIEM; and/or (c) on its part or any third party employed by it to plug in the pre-configured server and provide connectivity to such server will result in none of its assets being monitored by Exponential-e.

(b) **Threat Detection**

Exponential-e will alert and monitor the End User's estate for triggered threats and alert the Partner. This is a service consisting of a deployed USM sensor and the proactive monitoring of the Partner's estate, as defined in the SoW, on a 24x7x365 basis. The result of the monitoring consists of a web-accessed dashboard, which highlights alerts on a red, orange and green (RAG) priority basis. CSOC will provide the Partner with further intelligence via email-ticket about the incident in order to support remediation.

(c) **Internal Vulnerability Monitoring**

Exponential-e will provide vulnerability scans of the End User's estate, as defined in the SoW. This Service consists of a deployed USM virtual sensor and the proactive testing of the End User's monitored estate on a once per month 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 or third party responsible for the management of the estate in establishing the remediation action to take in all cases.

(d) **Monitored Compliance**

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

Change Management

Changes requested will be limited to a change of priority notification or change of monitored devices and will only be carried out during Normal Business Hours. In the case that a new device type is introduced to the CSOC Service, the CSOC won't be required to ensure that any agreed SLA of alerts, stated in the SoW, are met until a pre-agreed tuning period is completed, during this time the Partner/End User will regress to a Staging period instead of a Live status. Staging period being the period during which Exponential-e will monitor the SIEM to understand what changes, if any, is required to the CSOC Service before handover. The Partner is not entitled to any Service Credits for any failure by Exponential-e to meet the Service Level Agreement during the Staging period.

Access and Reporting

The USM System enables read-only access to the SIEM so that the Partner can obtain further information on a particular incident. The reports obtained following a vulnerability scan shall be shared with the Partner via an agreed method.

2. CSOC Service Demarcation Point (SDP)

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

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

3. 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. For the avoidance of doubt, notwithstanding any agreement by Exponential-e to delay the Service Commencement Date following the Partner's written request, the Service Commencement Date will be deemed to have occurred on the earlier of: (a) fourteen (14) days after the first log is ingested/collected by the USM System and (b) thirty (30) days from Order Form acceptance. Accordingly, the Annual Charge shall be deemed payable from that Service Commencement Date. Nothing in this clause shall oblige Exponential-e to agree to any delayed handover of this Service.

4. Service Level Agreement

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

Severity Level	Description
S1	A critical business service is non-operational impacting the Partner/End User 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 Partner/End User is experiencing failure or performance degradation that severely impairs operation of a critical business service; or the Partner/End User 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 Partner/End User 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 Partner/End User 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.*

5. Additional Terms applicable to the CSOC Service

5.1 In addition to the reasons set out in section 6.2 of the main body of this document, Exponential-e shall also have no liability for any failure to meet the Target Service Commencement Date and/or target service levels due to, or as a result of, any of the following reasons:

- Change management requirements affecting monitored devices
- Network or policy changes to a monitored device not performed by Exponential-e
- Loss of connectivity due to Partner/End User connectivity issues or Partner/End User managed issues
- Requirements which the Partner/End User must meet before the Service can be provided and during its provision as set out below ("Partner/End User Dependencies").

5.2 Partner/End User Dependencies

5.2.1 The Partner/End User shall ensure that:

(i) Each device covered by the Service has the appropriate full manufacturer's product licence and subscriptions for the duration of the Service. Software and devices that are considered end of life by the manufacturer are not covered by the Service; and

(ii) All devices must have full manufacturer's support for the duration of the Service; and

5.2.2 The Partner/End User accepts the following as a condition of Exponential-e providing the Service:

(i) Exponential-e is not responsible for resolving the Partner's/End User's Internet Service Provider (ISP) outages, or issues with the Partner's/End User's internal network or computing platform infrastructure where Exponential-e is not contracted to support those elements; and

(ii) It is the responsibility of the Partner/End User to ensure the log stream is directed at Virtual Monitoring Appliance for Service operation where applicable.