SERVICE SCHEDULE

SECURITY MANAGED SERVICES

This is a Service Schedule as defined in the Agreement. Where the Security Managed Services set out in this Service Schedule form part of the Services to be supplied under the Agreement, this Service Schedule forms part of the Agreement. In this Service Schedule, references to Clauses are to Clauses of the Agreement, and references to paragraphs are to the paragraphs of: (i) this Service Schedule; or (ii) whichever other document is specifically referred to. Defined terms that are used in this Service Schedule which are not defined in paragraph 1 below shall have the same meanings as set out in Schedule 1 of the Agreement.

1 Additional Definitions

In this Service Schedule the following definitions have the following meanings:

Acceptable Use Levels means the acceptable use levels identified in the table set out in paragraph 4.2;

Device means any device running a supported operating system that is managed under the Security Managed Service

Security Managed **Services** means the provision of technical services by the Supplier to configure, maintain and manage the security services provided under the Service Schedule;

Extended Waking Hours means standard daytime operating hours between 7:00 am and 7:00 pm on a Business Day;

Response Times means those response times identified as such in paragraphs 3.1 for the Supplier to respond to a ticket logged by the Company;

Service Hours means the hours identified in the tables set out in paragraphs 3.1;

Service Severity means the following priority levels as set out below:

Priority 1 **Catastrophic business disruption**, system or systems failure which is stopping the business from operating.

Priority 2 **Severe business disruption or user critical issue**, a critical user or group of users is unable to operate, or one or more critical system failures, or a critical system component has failed or is severely impaired but not impacting the business from operating.

Priority 3 **Business disruption or multiple user issue**, multiple users are experiencing an impacting issue, or a significant reduction in system performance.

Priority 4 **Minor business disruption or user issue**, a single user is unable to complete a task, or non-critical system is unable to operate or is degraded.

Priority 5 **Job or Task**, a request to undertake a defined job or task.

Waking Hours means standard daytime operating hours between 8:00 am and 6:00 pm on a Business Day.

2 Service Scope and Description

2.1 This Security Managed Service is provided to the Company for so long as the Agreement remains in force in accordance with the terms of the Agreement and the Supplier's Acceptable Use, security and access policies and procedures.

2.2 The provision of the Security Managed Service is subject to payment by the Company of the Supplier's Charges for installation and support services, as set out in the Order form or as subsequently agreed between the parties from time to time.

2.3 The provision of the Security Managed Service is subject to the Supplier delivering an 'audit and onboarding service' which will determine any remedial actions which would need to be addressed prior to the Security Managed Services going live. Any remedial actions will be discussed with the Company, and where the Supplier is required to undertake additional works as a result of the audit and onboarding service the Supplier will be entitled (in its sole discretion) to charge the Company. The audit and onboarding is included in the Charges listed in the Order form.

2.4 The provision of the Security Managed Service is subject to the Devices and the software running on the Devices (including the Operating System) being supported by the manufacturer or a Supplier approved 3rd party. Where the Device is not supported then the Supplier will provide the Security Managed Service on a reasonable endeavours basis and any agreed Response Times will not apply, and a failure of any kind will not be counted as a Business Critical Service Failure. The Supplier reserves the right to charge a 25% premium over the then list price for the Security Managed Service where the Device is not supported as defined in this paragraph. The Supplier may suspend support of relevant Devices under this clause without notice to the Company.

2.5 The Order form will specify the type of service being provided to the Company, including:

(a) Intune Managed Service

(b) Defender Managed Service

(c) Zero Trust Endpoint or equivalent

(d) BCN Managed Detection & Response (MDR)

(e) Security Awareness Service

(f) Vulnerability Management

(g) Dark Web Monitoring

2.6 The Supplier will (subject to Acceptable Use):

(a) where 'Intune Managed Service' is specified in the Order form:

(i) Setup a Device Management policy baseline

(ii) Provide bi-annual policy reviews, updates & maintenance

(iii) Setup, review and maintain Autopilot

(iv) Assess and implement new features, subject to Change Control and Clause 2.7(e)

(v) Setup an Application Management policy baseline

(vi) Provide monthly policy reviews, updates & maintenance

(vii) Upload & management of up to 20 well known applications

(viii) Provide enhanced reporting and insight into device & application estates

(ix) Provide quarterly report reviews & identification of improvement opportunities

(x) resolve or provide work arounds to technical incidents and problems; and

(xi) manage internal or external escalation of complex issues with the relevant vendors.

(b) where 'Defender Managed Service' is specified in the Order form:

(i) Provide bi-annual policy reviews, updates & maintenance

(ii) Assess and implement new features, subject to Change Control and Clause 2.7(e)

(iii) Endpoint Detection & Response, with automated device isolation

(iv) Provide enhanced reporting and insight into device & application estates

(v) Provide quarterly report reviews & identification of improvement opportunities

(vi) notify the Company of any endpoint device isolation and provide relevant vendor documentation to aid in remediation; and

(c) where "Zero Trust Endpoint Service" or "ThreatLocker" is specified in the Order form:

(i) manage an application whitelist

(ii) handle application whitelist requests from the Company's employees

(iii) handle temporary elevation control requests from the Company's employees; and

(iv) manage internal or external escalation of complex issues with the relevant vendors.

(d) where 'BCN MDR' is specified in the Order form:

(i) analyse & correlate event logs from Company's corporate devices, Microsoft's Entra ID Platform, & Firewalls (where specified)

(ii) raise security Incidents based on "Indicators or Compromise (IOCs)" in the Supplier's ITSM System

(iii) oversee automated actions including but not limited to:

(A) Malicious file removal

(B) Malicious process kill

(C) End User Device Isolation

(D) Server Isolation

(E) Blocking of compromised user accounts

(iv) where an impacted device or user account is covered by an existing Supplier service, the Supplier will perform additional manual actions including but not limited to:

(A) review of SOC reports in ITSM tickets;

(B) release of isolated devices;

(C) release of blocked identities.

(D) communication with the Company.

(v) provide regular service reporting including but not limited to:

(A) incidents identified as part of the Service;

(B) device vulnerabilities within the environment as identified by Microsoft Defender for Endpoint only.

(e) where “Security Awareness Service” is specified on the order form:

(i) assess the Customer’s employees on their cyber security proficiency;

(ii) setup & manage regular phishing campaigns;

(iii) setup & manage curated security training based on the results of (i) & (ii).

(f) where “Vulnerability Management Service” is specified on the order form:

(i) provide an initial vulnerability scan to identify & build a remediation plan for:

(A) end of life software;

(B) Out of scope software;

(C) Critical & high vulnerabilities;

(ii) scope an initial remediation plan

(iii) provide remediation for high & critical vulnerabilities that are in-scope through:

(A) applying updates

(B) configuration changes

(C) removing software

(D) other Supplier approved methods

(iv) provide an executive level report detailing vulnerabilities

(g) where “Dark Web Monitoring” is specified on the order form:

(i) scan the dark web for references to the Customer’s domain information or evidence of leaked credentials

(ii) alert a defined contact of any malicious findings

2.7 The Supplier will not:

(a) manage or support any of the Company's applications that are not specifically listed in this Service Schedule or specified in the Order form;

(b) support third party tools or environments, other than those specifically stated in this Service Schedule or specified in the Order form;

(c) provide any change management, any change will be managed through a defined and chargeable project;

(d) provide any support of devices running operating systems or applications that are not supported by the Supplier as defined in this Service Schedule or specified in the Order form;

(e) provide upload and management of applications that the Supplier deems to be subject to change management due to, but not limited to, application complexity, change risk, update complexity, or non standard deployment or application;

(f) provide training to the Company on the functionality and use of any supported operating systems or applications, unless specified in the Order form;

(g) remediate any device isolation, remediation maybe provided by other Services provided by the Supplier;

(h) where an impacted device or user account is not covered by an existing Supplier service, the Supplier will escalate to the Company;

(i) Unless the Order specifies Knowbe4 PhishER the Supplier will not investigate or manage any Phish Alert reports generated by users using the Outlook plug in provided by KnowB4

(j) support or manage the Company's active directory;

(k) provide forensic investigative services or analysis to determine the origin or method of any compromise identified as part of the service, or any additional in-depth investigation to remove a malicious actor from the Company's environment;

(l) provide remedial services to restore, repair or perform any activities to deal with any cyber-attack including but not limited to a virus attack, a phishing attack, or a crypto lock attack. Where the Company requests the Supplier to undertake any remedial services the Supplier reserves the right to charge the Company at the Suppliers prevailing rates or at a rate previously agreed, and the Company agrees to pay for such services prior to the Supplier commencing any works either by using call off time or by providing a PO, or;

(m) provide any other activity or service that is not set out in this Services Schedule.

2.8 The Company will:

(a) take responsibility for carrying out all deployment, configuration, and management of services not provided by the Supplier. The Supplier may take on these tasks at an

additional cost to the Company or bespoke professional services engagements, outside the scope of this End User Support Service;

(b) be responsible for ensuring that any data provided by the Company and that is hosted on devices that are either supplied or supported by the Supplier will not be in breach of any Law or contractual obligation of the Company; and

(c) ensure appropriate connectivity is provided and maintained (unless the Supplier is providing these connectivity services) to ensure the Supplier has access to provide the End User Support Services.

(d) Provide all required information in order for the Supplier to fully deliver the services as required

3 Response Times

3.1 The Supplier will use its reasonable endeavours to deliver the following Response Times for the 'services.

Service Severity	Service Hours	Response Times
Priority 1	Waking Hours or Extended Waking Hours	Within 60 minutes
Priority 1 (End User Out of Hours)	Outside Extended Waking Hours	Within 2 hours
Priority 2	Waking Hours or Extended Waking Hours	Within 2 hours
Priority 3 or 4	Waking Hours or Extended Waking Hours	Within 4 hours
Priority 5	Waking Hours or Extended Waking Hours	Within 8 hours

(a) Where a ticket is logged by the Company outside of the defined Service Hours the Response Time shall apply from the start of the Service Hours of the next Business Day.

(b) Where a ticket is logged during the Service Hours the clock shall not continue outside of the Service Hours, and shall resume during the Service hours of the next Business Day.

(c) Where the Supplier does not resolve or provide a temporary work around for a Priority 1 event within 10 Business Days the event will be classified as a Business Critical Service Failure, save where

(i) any part of the Service is provided by a third party and the third party is deemed by the Supplier to either wholly or partially be responsible for the Priority 1 event, or

(ii) the Company is deemed by the Supplier to either wholly or partially be responsible for the Priority 1 event, or

(iii) the Company has exceeded any Acceptable Use Levels or the Acceptable Use policy, or

(iv) where the Service that is affected by the event is not fit for purpose, out of support or end of life, and that the Supplier has previously informed the Company.

4 Acceptable use

4.1 The Services provided by the Supplier are subject to the Acceptable Use Levels. In the event the Company requests Services in excess of the Acceptable Use Levels the Response Times and Availability of such Services will be supplied either at an additional cost to the Company (at the Supplier's sole discretion) or with suspended Availability measures and Response Times.

4.2 The Acceptable Use Levels are set out in the table below.

Service	Acceptable Use Levels
Intune application update	No more than 20 known application updates applied in any 3 month period
Zero Trust Endpoint Service or ThreatLocker	Limited to 20 requests of any kind per user per month

5 Planned Maintenance

5.1 Save for a Force Majeure Event or in the case of an emergency, where the Supplier considers (in its sole discretion) that it is necessary to carry out planned maintenance activities that will affect or can reasonably be expected to affect the Company's operations, the Supplier shall notify the Company at least 48 hours in advance of the commencement of the planned maintenance detailing the nature of such maintenance to be carried out and the timetable for completion. Planned maintenance will be carried out in accordance with the Supplier's standard procedures which are available upon request by the Company. In the case of an Event of Force Majeure or an emergency, no advance notice is required.

5.2 During the period of any planned maintenance as detailed in paragraph 5.1, the Response Times will not apply.