Supplementary Terms for the supply of Security Monitoring Services

The Services set out in these Supplementary Terms shall be supplied by the Company to the Client on the terms and conditions set out in the Company's General Terms and Conditions and the terms and conditions of these Supplementary Terms. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

1.1 'Alarm' means a Security Incident that exhibits a pattern of potentially malicious activity that suggests an identified threat to the Monitored Infrastructure or violates acceptable use policies or circumvents standard security practices.

1.2 'Alert' means a Security Incident that is an observable occurrence in the Monitored Infrastructure, or, more broadly, the internet that may imply a potential threat to an information system or a potential compliance issue.

1.3 'Configuration' means the configuration of the Monitored Infrastructure, including Devices, installed software and all associated settings and or parameters.

1.4 'Device' means any device, including servers (virtual or physical), workstations, laptop computers, tablets and network equipment which is a constituent part of the Monitored Infrastructure.

1.5 'Emergency Maintenance' means any period of maintenance for which, due to reasons beyond its reasonable control, the Company is unable to provide prior notice of.

1.6 'End User' means a user of a Device.

1.7 'Hours of Cover' means the hours of cover set out in the Service Schedule.

1.8 'IT Equipment' means servers, workstations, laptops and other devices as set out on the Order.

1.9 'Malware' means software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system, including Trojan horses, viruses and ransomware.

1.10 'Monitored Infrastructure' means the IT Equipment and / or cloud based infrastructure to be monitored under the terms of this Agreement.

1.11 'Monitoring Agent' means the Company's monitoring agent which enables remote monitoring of the Monitored Infrastructure.

1.12 'Planned Maintenance' means any period of maintenance for which the Company has provided prior notice.

1.13 'Security Incident' means an Alarm or an Alert.

1.14 'Security Monitoring Services' means the security threat monitoring, detection, investigation, escalation, and Security Incident support services provided by the Company under the terms of the General Terms and Conditions and these Supplementary Terms, as described in the Service Schedule.

1.15 'Service Desk' means the Company's dedicated team of security specialists.

1.16 'Ticket' means a Security Incident report or Service Request that is logged on the Company's ticketing system by either the Client or the Company.

2. TERM

2.1 This Agreement shall come into effect on acceptance of the Client's Order by the Company and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for the Minimum Term as set out in the Order.

2.2 This Agreement shall continue to run after the expiry of the Minimum Term (or subsequent Additional Term) for an Additional Term. The duration of the Additional Term shall be the same as the Minimum Term unless otherwise agreed in writing. In the event that:

2.2.1 The Client serves not less than ninety days' notice prior to the end of the current term to terminate this Agreement in accordance with clause 11 of the General Terms and Conditions or clause 9 hereof, this Agreement shall terminate at the end of the Minimum Term or any Additional Term thereafter;

2.2.2 If the Client fails to serve notice to terminate, the Agreement shall continue in force for an Additional Term.

3. PROVISION OF SERVICES

3.1 Security Monitoring Services provides real time monitoring to detect and respond to malicious code, Malware, malicious logins, suspicious activity, intrusions and other security threats.

3.2 The Company provides two Security Monitoring Services, Office 365 Monitoring and Log Security Monitoring, which are provided remotely and include:

3.2.1 Monitoring and Security Incident detection;

3.2.2 Security Incident Triage;

3.2.3 Escalation of Alarms to the Client;

3.2.4 Reporting.

3.3 During the term of this Agreement, the Company shall be entitled to make alterations to the Security Monitoring Services. Such alterations may result in temporary disruption to the availability of the Security Monitoring Services and the Company will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

3.4 The Company cannot guarantee and does not warrant that the Security Monitoring Services shall result in the Monitored Infrastructure operating free from Malware, malicious logins, intrusions or other threats.

3.5 The Company provides Security Monitoring Services under the terms; and

3.5.1 The Company shall use reasonable endeavours to provide the Security Monitoring Services 24 x 7 x 365;

3.5.2 The Company cannot guarantee and does not warrant that the Security Monitoring Services will be free from interruptions, including:

a) Interruption of the Security Monitoring Services for operational reasons and temporary degradation of the quality of the Security Monitoring Services;

b) Interruption of the connection of the Security Monitoring Services to other network services provided either by the Company or a third party; and

c) Any such interruption of the Security Monitoring Services referred to in this sub-clause shall not constitute a breach of this Agreement.

3.6 Although the Company will use reasonable endeavours to ensure the accuracy and quality of the Security Monitoring Services, the Security Monitoring Services are provided on an "as is" basis and the Company does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for the Client's purpose of the Security Monitoring Services.

4. ACCEPTABLE USE

4.1 The Client agrees to use the Security Monitoring Services in accordance with the provisions of this Agreement, any relevant Service literature and all other reasonable instructions issued by the Company from time to time.

4.2 The Client acknowledges that it responsible for all data and/or traffic originating from the Monitored Infrastructure.

4.3 The Client shall not, and shall ensure that its End Users do not act in any way which threatens the security or integrity of the Security Monitoring Services.

4.4 The Client agrees to immediately disconnect (and subsequently secure prior to reconnection) Devices generating data and/or traffic which contravenes this Agreement upon becoming aware of the same and/or once notified of such activity by the Company.

4.5 Subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, the Client shall indemnify the Company against any third-party claims arising from the Client's breach of the terms of this clause 4.

5. CLIENT'S OBLIGATIONS

During the term of this Agreement, the Client shall:

5.1 Ensure that user-names, passwords and personal identification numbers are kept secure and:

5.1.1 Unless otherwise protected by two-factor authentication, on a regular basis, change access passwords for all Devices that in the Client's reasonable opinion may be liable to access by unauthorised persons.

5.2 Accept that is the Client's sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training to prevent the introduction of Malware into the Monitored Infrastructure.

5.3 Provide permanent access to the Public Internet, as required for the correct functioning of the Security Monitoring Services.

5.4 Provide reasonable assistance to the Company including helping to trouble-shoot technical issues within the Monitored Infrastructure and in any services provided to the Client by third parties that may affect the delivery of the Security Monitoring Services.

5.5 Provide the Company with accurate and up-to-date information including:

5.5.1 The name, email, landline, and mobile numbers for all designated authorised Client points of contact;

5.5.2 Device and credential information as required by the Company;

5.5.3 Planned changes to the Monitored Infrastructure;

5.5.4 Any scheduled maintenance, network or system administration activity that could affect the Company's ability to perform the Security Monitoring Services.

5.6 Maintain current warranty and / or maintenance and technical support contracts with Client's software and hardware vendors for any Devices that are covered by the Security Monitoring Services.

5.7 If a Security Incident is assigned to the Client after analysis by the Company, the Client shall be responsible for the ownership of the Security Incident until such time as it is resolved or otherwise closed by the Client or is passed back to the Company for further action.

5.8 Use reasonable endeavours to execute the Client actions within the timescales set out in sub-paragraph 7.4 of the Service Schedule.

5.9 Ensure that all times either the primary or secondary Client contact is available by telephone / mobile telephone to receive escalations from the Company.

5.10 Acknowledge that the Company's supplier may contact the Client directly on behalf of the Company during the analysis, investigation of a Security Incident.

5.11 Not resell or sub-licence the Security Monitoring Services.

6. THE COMPANY'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Client of its obligations hereunder, the Company shall:

6.1 Provide the Security Monitoring Services set out in the Order and described in the Service Schedule.

6.2 Provide a Service Desk which will be available to provide assistance with Security Incidents during the Hours of Cover set out in the Service Schedule.

6.3 Monitor the Monitored Infrastructure 24 x 7 x 365 and proactively investigate and respond to all Security Incidents.

6.4 The Company will provide investigation, analysis, escalation and support for all Security Incidents that are detected by the Services, including:

6.4.1 Ensuring that Security Incidents are detected and escalated in a timely manner;

6.4.2 Providing the focal point for organisational security issues;

6.4.3 Responsibility for event analysis and investigation to determine if Security Incidents warrant Alarm classification;

6.4.4 If a Security Incident is classified as an Alarm by the Company, responsibility for tracking the Alarm with the Client through to final resolution;

6.4.5 Performing Security Incident triage to include determining scope, urgency, and potential impact, and will identify specific vulnerabilities and make recommendations to allow for remediation.

7. Clause Intentionally Unused

8. GENERAL

8.1 The Company may perform Planned Maintenance that may limit the availability of the Security Monitoring Services. The Company will use reasonable endeavours to schedule such maintenance to minimise disruption to the Client.

8.2 The Company may be unable to provide prior notice of any Emergency Maintenance that may limit the availability of the Security Monitoring Services, but will endeavour to minimise the impact of any such maintenance on the Client.

8.3 If the Company carries out work in response to a Security Incident which is found by the Company to be caused by an act or omission of the Client, the Company shall be entitled to charge the Client accordingly at its prevailing rate.

8.4 It is the Client's sole responsibility to ensure that the receipt by the Client of Security Monitoring Services will not breach the terms of any cyber-insurance policy that the Client has in place.

8.5 If the Client is contacted by the Company and requested to make a change to the Configuration of the Devices, it is the Client's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.

8.6 If the Company resets any passwords during the execution of the Security Monitoring Services, it shall be the Client's sole responsibility to change such changed passwords and ensure that such changes are compliant with any security policy that may be in effect.

8.7 The Client acknowledges that if it elects not to take advice given by the Company in relation to the security and performance of the Monitored Infrastructure, there may be a resulting risk to the integrity of the Monitored Infrastructure and that the Company shall not be liable for any degradation in integrity resulting from such decision and that any additional costs incurred by the Company resulting there from will be charged to the Client.

8.8 The Client hereby consents to the Company and its partner remotely accessing any Devices in the Monitored Infrastructure for the sole purpose of providing the Services under the terms of this Agreement.

9. TERMINATION

9.1 In addition to the provisions of clause 11 of the General Terms and Conditions, this Agreement may also be terminated by either party by giving the other not less than ninety days' notice in writing to terminate on the last day of the Minimum Term or last day of any Additional Term thereafter.

10. CHARGES AND PAYMENT

10.1 The Company shall raise invoices according to the schedule set out on the Order.

10.2 Invoices for Recurring Charges shall be raised in advance of the relevant period. The invoicing period is set out in the Order.

10.3 In addition to Charges contemplated in sub-clause 10.1, the Company shall be entitled to charge the Client for:

10.3.1 The ad hoc supply of any Services that are requested by the Client but not set out on the Order;

10.3.2 Reasonable expenses.

10.4 The Company shall commence charging for the Security Monitoring Services from the RFS Date, regardless of the date on which the Client commences use of the Security Monitoring Services. If the RFS Date does not correspond with the Company's invoicing period as set out in the Order, the Company shall charge the Client at a pro-rata rate for the first invoicing period.

10.5 The Client acknowledges that the Charges for the Minimum Term are calculated by the Company in consideration inter alia of the setup costs to be incurred by the Company and the length of the Minimum Term offered.

10.6 The Client may at any time, increase the number of Devices to be monitored by raising a supplemental Order and the Client acknowledges that at the price charged by the Company for monitoring additional Devices may differ from any previous prices or quotations provided by the Company.

10.7 The Client agrees that it shall be liable for termination Charges if this Agreement is terminated by:

10.7.1 The Client terminating this Agreement for convenience prior to the end of the Minimum Term or Additional Term, whereupon the Client shall be liable for the Charges payable for the remainder of the current term;

10.7.2 The Company terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Client's un-remedied breach of the terms of this Agreement, whereupon the Client shall be liable for the Charges payable for the remainder of the current term.

10.8 The Client shall not be liable for termination Charges if this Agreement is terminated by:

10.8.1 The Client at the end of the Minimum Term or Additional Term PROVIDED THAT the Client properly serves written notice to terminate, in accordance with clause 9 of these Supplementary Terms and clause 11 of the General Terms and Conditions;

10.8.2 The Company at any time if it can no longer provide the Services or part thereof;

10.8.3 The Client by reason of the Company's un-remedied or repeated breach of the terms of this Agreement.

11. LIMITATIONS AND EXCLUSIONS

11.1 Whilst the Security Monitoring Services is intended to proactively identify most Malware, malicious logins, suspicious activity, intrusions and other security threats, the Company does not warrant and

cannot guarantee that the Security Monitoring Services will identify all security threats and shall not be liable for any losses, damages or costs arising from such unless such result directly from the negligence of the Company.

11.2 Public Internet connectivity that is required to enable the Security Monitoring Services is not provided by the Company under the terms of this Agreement.

11.3 The Company shall not be liable for any damages, costs or charges arising from damage to, or theft of data that is transmitted from the Client's site to the Security Monitoring Services via the Public Internet, nor for any other losses that occur due to reasons beyond its reasonable control.

Service Schedule

This Service Schedule describes all of the Security Monitoring Services that are supplied by the Company. The specific Services described in paragraphs 3 and 4 shall be provided as set out on the Order.

1. Service Overview

1.1 The purpose of the Security Monitoring Services is to identify threats to the Monitored Infrastructure as soon as reasonably possible and take the necessary actions to mitigate the impact of the threat. The Company achieves this objective by:

- Real time monitoring the Monitored Infrastructure and the network traffic to and from it
- Analysis of suspicious and potentially malicious activities
- Notifying the Client when confirmed threats have been identified
- Suggesting remediation actions to the Client
- Ongoing education of the Client, via the release of threat advisories
- Ongoing review of the global threat landscape

1.2 Security Incidents are detected by automatically analysing data from a number of sources (sub-paragraphs 3.2 and 4.2 provide more detail) followed by manual triage to determine categorisation, severity and priority (sub-paragraph 7.4 provides further detail).

1.3 When an Alarm is identified, the Client will be contacted by the method set out in sub-paragraph 7. 4.

2. Service Initiation

- The Company will review and where necessary make appropriate changes to the IT Equipment's configurations to ensure that the Services detailed in this Service Schedule can be delivered effectively. This includes changes to the configuration of Microsoft Windows event logs, Microsoft Windows, Exchange and SQL Server services, anti-virus and backup software
- The Company will agree with the Client a number of standard procedures that the Company will follow when receiving requests from the Client for adding, removing or changing access to the Client's network. This will include but is not limited to creating, deleting, or amending user accounts, security permissions, and folders and shares
- The Company will inform the Client if the Company is unable to configure any components the IT Equipment to provide the necessary alerting and will agree a suitable alternative with the Client
- Implement account and user setup for the Services
- Create a "Challenge / Response" account verification policy for the Services

3. Log Security Monitoring Service

3.1 The Company will provide this Service if such is set out on the Order. Log Security Monitoring and intrusion Monitoring Agents are installed at one or more strategic locations in the Client's Local Area Network, generally where traffic is most likely to be vulnerable to attack which is typically at points of traffic ingress and egress. The Service correlates suspicious events and as appropriate generates Security Incidents that are then reviewed by the Company's team of security experts. The service operations centre generates reports and raises Alarms when threats are identified.

3.2 Data Sources

The Company's Log Security Monitoring Service collects audit, activity and security logs from:

- Applications – Logs from application and web servers
- Servers – Logs from Windows and Unix operating systems

- Endpoints – Logs from anti-virus and EDR solutions
- Cloud – Logs from Azure event hub, AWS, etc.

Data sources are updated as the threat landscape evolves and Microsoft's capabilities advance.

3.3 Security Incidents

The Log Security Monitoring Service checks for a range of Security Incidents, including the following:

Security Incident	Example
Administrator Actions	An MFA device was deactivated
Anomaly Detection	Credential dumping
Authentication	VPN logon from outside specified country
Entity Behaviour	Failed account activity to a recently disabled account
Intrusion Detection	Server instance communicating to the same, potentially nefarious external IP address
Intrusion Prevention	IPS exploit detection
Malware Detection	Known Malware File Captured
System error	Multiple HTTP client-side errors from the same IP address
Status Monitoring	Disruption of security telemetry
Security Orchestration	Traffic to/from Tor networks
User Behaviour	Multiple account lockouts

4. Office 365 Monitoring Service

4.1 The Company will provide this Service if such is set out on the Order. Office 365 Monitoring automatically reads and analyses Microsoft Azure and Microsoft 365 logs. The Service correlates suspicious events and as appropriate generates Security Incidents that are then reviewed by the Company's team of security experts. The service operations centre generates reports and raises Alarms when threats are identified.

4.2 Data Sources

The Company's Office 365 Monitoring Service collects Microsoft audit, activity and security logs from:

- Azure event hub
- Microsoft management API

Data sources are updated as the threat landscape evolves and Microsoft's capabilities advance.

4.3 Security Incidents

The Company's Office 365 Monitoring Service checks for a range of Security Incidents, including the following:

Security Incident	Description
Brute Force Access Attempt	Detects simultaneous failed authentications to Office 365 with the same account from different countries. This may indicate stolen credentials unless it is an administrative account and is supposed to be accessed by administrators from multiple countries.
Brute Force Access Successful	Detects the condition where an account has multiple authentication failures followed by a successful authentication within a short time window
Successful Foreign Login	Detects an Office 365 logon from a suspicious country list
Multifactor Authentication Disable	Detects when multifactor authentication has been disabled on an account
Suspicious Email Forwarding	Detects if a mailbox rule was created, modified, or deleted on Office 365. This could be an indicator of an account breach where an adversary has created a rule to monitor conversations or ex-filtrate data.
MS ATP Anti Phishing Disabled*	Detects when a user with escalated privileges or a script has disabled an anti-phishing rule in Office 365. This unusual event could indicate malicious activity warranting investigation.
MS ATP Malware Filter Policy Disabled*	Detects when a user with escalated privileges or a script has disabled a Malware policy in Office 365. This unusual event could indicate malicious activity warranting investigation.
MS ATP Malware Filter Disabled*	Detects when a user with escalated privileges or a script has disabled a Malware filter in Office 365. This unusual event could indicate malicious activity warranting investigation.
MS ATP Safe Attachments Disabled*	Detects when a user with escalated privileges or a script has disabled “Safe Attachments” in Office 365. This unusual event could indicate malicious activity warranting investigation.
MS ATP Safe Links Disabled*	Detects when a user with escalated privileges or a script has disabled “Safe Links” in Office 365. This unusual event could indicate malicious activity warranting investigation.
* subject to the Client’s subscription to MS ATP	

5. Service Desk

5.1 The Company’s search and detection technology is backed by its team of certified security specialists who provide the following services:

- Proactively research threats
- Use a combination of machine and human analysis to review and scrutinise Security Incidents as they arise
- Alarms / Alerts are escalated to the Client according to its designated escalation call tree.
- Respond to Tickets raised by the Client
- Provide advice regarding specific Alerts and Alarms
- Provide remote remediation assistance
- Carry out password resets (in response to specific requests from the Client)

5.2 The Hours of Cover for the Service Desk are 24 x 7 x 365.

5.3 The Client may contact the Service Desk by one of the methods provided by the Company at the commencement of this Agreement.

6. Reporting

The Company will provide monthly reports which will identify:

- An executive overview, summarising Security Incidents that confronted the Client in the reporting period
- Security Incident details with relevant elements such as: date of discovery, severity, network type, source date, remediation, and source URL
- Threat advisories, a list of advisories that the Company publishes periodically
- Remediation status including all remediation actions including Security Incident identifier, source date, source URL, type, status, and activity log
- Data Sources, including Information about current data sources (servers, firewalls, etc.)
- Source Types, including the number of threats that come from each source type
- The number of threats of each Security Incident type

7. Service Level Agreement

7.1 The Company shall provide the Monitoring Service 24 x 7 x 365 with an availability target of 99.5%.

7.1.1 The availability target does not include non-availability due to Planned Maintenance.

7.2 The Company will aim to respond to failures in the Monitoring Services as described below:

	High Priority	Medium Priority	Low Priority
Description	Major Service Outage, for example entire Monitoring Services outage	Significantly Degraded Service, for example the Monitoring Services is impaired but functional	Slightly Degraded Service, for example Monitoring Services are suffering from performance degradation, limited access or intermittent failure
Escalation Method	Telephone / Email / Ticket	Ticket	Ticket
Target Response Time	2 hours	9 hours	14 hours
Overall response target	95% in any month	95% in any month	95% in any month

7.3 The Company will aim to respond to action service requests as described below:

Service Request Type	Target Resolution Time
Add, Change, Remove up to five endpoints	4 Working Days
Configuration Changes	8 Working Days
Provision of new Monitoring Services	15 Working Days

7.4 The Company will aim to escalate Alarms to the Client as described and within the timeframes described below:

	High Priority	Medium Priority	Low Priority
Description	High risk events that have the potential to cause severe damage to the Client's infrastructure. Examples include successful data leakage, malware propagation, successful brute force login and successful communication between an item of IT Equipment and an external rogue server	Medium risk events that may cause some damage to the Client's infrastructure. Examples include unauthorised local scanning, outbound connection to a TOR network, multiple distinct IPS events from the same source, Active Directory modifications, malware detection on a single item of IT Equipment	Low risk events that have the potential to cause minor damage to the Client's infrastructure. Examples include discovery and vulnerability scanning, information-gathering scripts, five or more brute-force login attempts, SQL injection attempts
Escalation Action	The Company will escalate to the nominated Client contact by telephone, and will provide information on the type of threat and guidance on mitigation activities. If the Company is unable to contact the primary Client Contact, an attempt will be made to contact the secondary contact	The Company will escalate to the nominated Client contact by raising a Ticket, and will provide information on the type of threat and guidance on mitigation activities	The Company will escalate to the nominated Client contact by raising a Ticket, and will provide information on the type of threat and guidance on mitigation activities
Escalation Method	Telephone and Ticket	Support Ticket	Support Ticket
Backup Escalation Method	Mobile phone	N/A	N/A
Target Response Time	20 minutes	1 hour	8 hours
Client Actions	Review the Alarm / escalation when notified and take action immediately	Review the Alarm / escalation and take appropriate action within 8 – 12 hours of being notified and advise the Company of actions taken	Review the Alarm / escalation and take appropriate action within 12 – 24 hours of being notified and advise the Company of actions taken

7.5 Failure by the Company to meet the targets set out in this paragraph 7 shall not be deemed a breach of this Agreement.

8. Complaint Handling

8.1 If dissatisfied with any Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the escalation path:

Escalation Level	Role	Contact Details
1	Service Desk Engineer	0203 907 9570
2	Service Desk Team Leader	0203 907 9567
3	Head of Delivery	0203 907 9561

8.2 The Company will respond to complaints within three Working Days.