Cyber Security Services - Service Specific Terms (SST)

These Service Specific Terms set out the terms and conditions which apply to Cyber Security Services.

1. PROVISION OF SERVICES

1.1 These Service Specific Terms shall govern the provision of the Cyber Services by Supplier, and the consumption of the Cyber Services by Customer.

1.2 Supplier reserves the right to withdraw or modify any Service Description without notice, to the extent necessary to ensure compliance with any regulatory or legislative requirement, or in the interest of maximising the effectiveness of its services, provided that such withdrawal or modification does not have a material adverse effect on a Service.

1.3 The Customer acknowledges that, for certain Services provided under this agreement, Supplier is reliant on variable pricing arrangements with third party suppliers who may change their charges to SCC from time to time. Consequently Supplier shall be entitled to increase or decrease the Charges to pass on the respective increase or decrease in charges payable by Supplier specifically to the third party providers of the following: (a) data centre colocation or hosting (including private cloud) services due to price increases from the applicable supplier of racks or electricity/power; (b) network connectivity (including in connection with SCC's private cloud Services) and telecommunications provided by network carrier(s); and (c) software used by SCC as a managed service provider in the delivery of our Services.

2. MSP SOFTWARE

2.1 Where the Cyber Security Services require the installation by us of MSP Software in your IT environment:

(a) we may deploy such MSP Software, and any updates, patches, new releases and new versions received from the licensor from time to time;

(b) we shall also use reasonable discretion to decide which patches, updates, releases or new versions to install; and

(c) we shall use reasonable endeavours to check MSP Software releases and versions are in working order prior to installation and you shall provide the necessary level of assistance in implementation and testing thereof.

2.2 You agree to be bound by and comply with the terms of the relevant end user licence or similar agreement for any MSP Software used to receive the Cyber Security Services (the "EULA").

2.3 You shall ensure that we are licensed to use the MSP Software that you have agreed to provide access to for us to provide the Cyber Security Services, as set out in the Technical Specifications.

2.4 You acknowledge that the MSP Software includes a monitoring capability that sends anonymous statistics about performance, device utilisation and network size remotely to us. Save to the extent required for the effective performance of the Cyber Security Services, we will not use such technical information in a form that could in any way identify you.

3. SOFTWARE MAINTENANCE

3.1 Where your software is maintained by us, as set out in the Technical Specifications, you acknowledge and agree that:

(a) we will refer the software Incident directly to the manufacturer or approved support partner where it is not possible for us to effect Incident resolution; and

(b) where appropriate and possible to do so, we will utilise the software support, fault diagnosis and fault resolution support we receive from our own third party software support arrangements for your benefit.

4. CUSTOMER OBLIGATIONS

4.1 Except as agreed by the Supplier as part of the Cyber Security Services, you shall:

(a) manage and keep up to date with any maintenance and technical support contracts with your software and hardware vendors for any Monitored Assets;

(b) interact with vendors and/or manufacturers of the Monitored Assets to resolve any issues related to feature limitations or performance which hinder or delay the provision of the Cyber Security Services;

(c) notify us of any changes to Monitored Assets, equipment, software, network connections, or data feeds that could impact our provision of the Cyber Security Services. Any assistance required by us to remedy or resolve such impacts shall be chargeable;

(d) be responsible for obtaining and maintaining all equipment, software and network connections necessary to access and use the Cyber Security Services, and for paying any applicable third party fees and charges incurred to access and use the Cyber Security Services;

(e) provide Supplier with access to your IT Infrastructure via a secure broadband link operating at the industry accepted bandwidth for the Cyber Security Services and the purposes of remote diagnostics (if required);

(f) ensure that we can access your IT Infrastructure to the extent necessary to provide the Cyber Security Services, including providing secure remote access or screen sharing systems;

(g) obtain necessary permissions or services from third parties (including the providers of your internet access and other data communication services) to ensure we can deploy our equipment or MSP Software for the Cyber Security Services, and allow us, with your approval and at your expense, to make reasonable service requests from those third parties; and

(h) inform us promptly in the case of a denial-of-service attack or distributed denial-of-service attack and, in the event of any such incident, we will work with you to assess the situation as quickly as possible and discuss and agree on appropriate action in respect of the Cyber Security Services in such circumstances (including the possibility of suspending the Cyber Security Services).

4.2 Where the Cyber Security Services include incident management, you shall:

(a) provide all relevant information, including a detailed description of the fault or defect, the procedures required to replicate the issue, and any additional information which may help in the diagnosis of the fault or defect (e.g. network configuration details);

(b) provide us with access to your IT Infrastructure via a secure broadband link operating at the necessary bandwidth for the purposes of remote diagnostics should such capability be required; and

(c) inform and keep us updated regarding any of the critical information associated with any Security Incident.

5. CUSTOMER CONSENTS AND AUTHORISATIONS

5.1 As necessary for the performance of the Cyber Security Services and to the extent not prevented by applicable law, you authorise us to:

(a) access any IT Infrastructure relevant to the Cyber Security Services;

(b) circumvent or overcome technological or physical measures which have been implemented to protect against unauthorised access to any part of your IT Infrastructure and to use or provide technology to achieve any such circumvention;

(c) intercept telecommunications and electronic communications;

(d) share information or take such actions with respect to any part of your IT Infrastructure as required by law enforcement authorities or regulatory authorities or applicable law. In such cases we will use reasonable endeavours to notify you in advance, where we are permitted by such law enforcement and/or regulatory authorities or applicable law to do so;

(e) retain for our own business purposes any indicators of security compromise, malware, vulnerabilities or other anomalies found as part of, or related to the performance of the

Cyber Security Services and to anonymise and aggregate all data relating to the same to develop, provide and improve our Services; and

(f) take any other actions which may reasonably be required for us to provide the Cyber Security Services to you.

5.2 You represent, warrant, and agree that you have and will maintain all permissions, consents, licences, rights, or authorizations necessary for us to carry out the acts authorised in clause 5.1 in our performance of the Cyber Security Services.

5.3 You shall defend, indemnify and hold us harmless from and against all losses (including any actions, claims, costs, damages, expenses, fines, liabilities, penalties and sanctions, amounts paid in settlement, out-of-pocket expenses and interest) together with all reasonable legal expenses that we incur as a result of any action, claim, demand, proceeding, filing, objection or complaint from a third party or relevant authority arising directly or indirectly from your breach of clause 5.2.

6. EXCLUSIONS

6.1 You must ensure that upgrades, fixes, and patches, *etc*. are installed for all software you **use in** your IT environment unless such services are expressly stated to be delivered by us as part of the Cyber Security Services or any other Services, including a professional services engagement with us.

6.2 We shall use reasonable endeavours to carry out the Cyber Security Services in a manner that causes no significant impact or disruption to you, however you acknowledge that there is an inherent risk that the Cyber Security Services could result in operational or performance degradation, breach of your internal policies or industry standards, or otherwise impair or result in loss or damage to your IT Infrastructure.

6.3 It is not possible to provide a definitive Incident resolution timescale or target for software problems and faults (due to their sometimes complex nature), therefore Incident resolution will be provided on a reasonable endeavours' basis only.

6.4 Without limitation, the following activities are out of scope and are not provided by us as part the Services:

(a) training in the use of any upgrades, updates, or new releases to the MSP Software;

(b) any legal advice, expert testimony, or litigation support services of any kind or any services involving the collection of physical evidence, chain of custody collection of evidence for criminal or civil litigation purposes, or for admission in court, or providing evidence lockers or 'chain of custody' collection of evidence; and

(c) patching shall only be provided to the extent we have expressly agreed to provide it as part of the Cyber Security Services or otherwise as part a different Service provided by SCC.

6.5 We will have no responsibility or liability for:

(a) faults or errors in MSP Software resulting from:

i. changes to the MSP Software, except for changes implemented by us or on behalf of us;

ii. failure to use MSP Software in accordance with the EULA or instructions for its use;

(b) faults in the hardware or any equipment on which the MSP Software is used (other than our own hardware or equipment);

(c) damage or loss caused to your IT Infrastructure or operations as a result of fault, error, virus or other failure in the MSP Software and any other software updates, patches and upgrades released by the vendor;

(d) unauthorised use of the MSP Software by you or use otherwise than in accordance with the SCC MSA Order Form or other applicable ordering document; and

(e) circumstances in which you have not implemented the updates and upgrades supplied or recommended to you by us or the manufacturer.

6.6 We shall provide the Services exercising that degree of skill, care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced provider engaged in the same type of undertaking under the same or similar circumstances and in accordance with the Service Description (and we shall be liable for any failure to do so subject always to the terms and conditions of this Agreement). But you acknowledge and agree that we cannot ensure that:

(a) you will be protected against all threats and attacks relating to your IT Infrastructure, or

(b) all threats and attacks can be mitigated or resolved to a particular timescale or even at all.

6.7 We cannot guarantee that there will be no loss, damage or interruption to your IT Infrastructure or data due to threats inherent in the use of network connections, telecommunications links, facilities and internet access.

7. DEFINITIONS

7.1 In this Cyber Security Service Specific Terms and associated Cyber Security Services service descriptions, the following terms shall have the following meanings:

Term	Meaning
Collector	Means a tool that is deployed within the Customer's IT Infrastructure to collect event data to be ingested into the Solution.
Customer Controlled Equipment	Means equipment (within the Customer's IT Infrastructure) owned by Customer or its suppliers, used in the provision of the Services to Customer.
Cyber Security Incident	Means an Event that triggers either one or more regulatory regime correlation directives or built in SIEM correlation directives, thereby creating an alarm within the SOC that is subsequently identified by the SOC as an organised attack.
Cyber Security Services	Means the specific cyber security services to be provided by Supplier to Customer under an agreement as listed in the relevant SCC MSA Order Form or other applicable ordering document
Data Retention	Means the duration of time that the event data is retained within the Solution as specified in the Technical Specification.
Emergency Change	Means a change that must be introduced as soon as possible to maintain system availability, integrity or confidentiality.
Endpoint	Means a computer device with an operating system, used by an individual End User.
Endpoint Detection and Response or EDR	An endpoint security solution that continuously monitors and responds, using intelligence systems, to mitigate and protect against cyber security threats.
End User	Any individual or entity that directly (or indirectly through another user) accesses or uses a system or Service through the Customer.
Event	Means a security event notification sent by a Monitored Asset as a consequence of the data that has been ingested by the Solution.
IT Infrastructure	Means any existing information technology (IT) infrastructure, environments, hardware, software, processes, policies and any

Term	Meaning
	other Customer provided elements which are integral to the successful provision of the Cyber Security Services.
Management Server	Means the centralised management system that aggregates and correlates information gathered by the Collector and provides a single point of reference to us for its monitoring, management, reporting and administration functions.
Monitored Assets	The environment, system, service or End User which we monitor on behalf of a Customer as specified in the Technical Specification.
MSP Software	Means the managed service provider (MSP) software (including related documentation and any future updates provided by us, your other suppliers, or the manufacturer) that is used by us in the performance of Services or that is provided by us for use by you as part of the Services for which title to the software licence remains with us or the manufacturer and does not transfer to you (excluding any software that is purchased by you).
National Cyber Security Centre	Means the information security arm of GCHQ in the United Kingdom.
Security Hardware	Means the hardware on which the security software resides.
Security Incident	An event raised by us due to an alert received via our tools or the Solution and categorised by us as such.
Security Incident and Event Monitoring or SIEM	Means a service that provides monitoring of Events generated by server and network infrastructure.
Security Operations Centre or SOC	Means the combined staff and function provided by us at one or more locations by which security monitoring and management is performed on your behalf by us pursuant to the order.
Security Testing	Means the process of performing security testing of your system as defined in the Technical Specification.
Solution	The combination of the technology, underpinning hardware and software, the professional services and the managed services that Supplier uses to provide the Cyber Security Services and other services.
Supplier Equipment	Means equipment owned by us or our suppliers, used in the provision of the Services to you.
Zero Day Vulnerability	Means a vulnerability in a system or device that has been disclosed but is not yet patched.