

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

1. APPLICATION

- 1.1 This Schedule, which contains a description of Managed Security Support, forms part of the Agreement entered between the Parties for the provision of Services together with the General Conditions and other documents listed at clause 1.4 of the General Conditions.
- 1.2 Definitions and interpretations that are specific to this Schedule are set out in **Annex 1** and apply in addition to the definitions and interpretations set out in **Schedule 1 (Definitions)** of the General Conditions.
- 1.3 Where a Scope of Works (“SOW”) is agreed between the parties, and signed by the Customer, it shall form part of this Schedule. In the event of express conflict between the SOW and this Schedule, the SOW shall take precedence.

2. SERVICE DESCRIPTION

- 2.1 Where stated on the Order and/or SOW, the Supplier shall provide support for the Supported Equipment as detailed in this Schedule (“**Managed Security Support**”). If the Supplier provides **Standard Security Support, Schedule 4.6(A)** shall apply and not this Schedule.
- 2.2 The Supplier shall provide the Customer with:
 - 2.2.1 access to MyPortal and contact details for the Service Desk;
 - 2.2.2 remote Fault management support in accordance with paragraphs 2.10 to 2.31; and
 - 2.2.3 facilitate any claim made under a Third-Party Supplier warranty and/or support contract on behalf of the Customer;
 - 2.2.4 System Monitoring;
 - 2.2.5 Implementation and Configuration of Supported Equipment;
 - 2.2.6 Elective Change Management;
 - 2.2.7 System Back Ups and Recovery in the event of a disaster;
 - 2.2.8 Pro-active patch management;
 - 2.2.9 End User Support;
 - 2.2.10 Monthly report; and
 - 2.2.11 Quarterly advisory sessions.

INITIAL CONFIGURATION

- 2.3 The Customer shall provide all necessary Supported Equipment prior to the Commencement Date unless such Hardware or Software is being provided by the Supplier pursuant to an Order.
- 2.4 Where the Customer does not purchase the Supported Equipment from the Supplier, the Customer shall provide suitable alternative servers and infrastructure and must ensure that they meet the minimum requirements, including but not limited to all port requirements. It is also the Customer’s responsibility to make any required port access changes.
- 2.5 Subject to compatibility, the Supplier shall configure the Customer’s servers and infrastructure to host the specified Managed Security Support. The Customer shall obtain the requisite Hardware and Software and will provide the Supplier with an account to access the management consoles with sufficient privileges to perform the required administration.

- 2.6 The Customer must ensure that the existing Third-Party Supplier AV solutions are centrally managed and any tamper protection can be switched off on all devices, before the Supplier is able to migrate if an AV product is included.
- 2.7 Server and proxy reboots/downtime should be expected with any upgrade processes performed by the Supplier. The Supplier shall agree and notify the Customer of any planned upgrades/downtime on the Customer Network.
- 2.8 For product or Vendor specific requirements and obligations please see **Annex 2 (Sophos) or Annex 3 (Microsoft)**.

MYPORTAL

- 2.9 MyPortal provides the Customer with important information about its account, systems, and services. It enables the self-service management of the Services providing, status updates and responses to assist in the monitoring and reporting of the Supported Equipment.
- 2.10 The Supplier shall provide to the Customer’s designated administrator a unique login ID and password to access the Customer’s account in MyPortal. As a designated administrator, access to MyPortal can be enabled for others, including control of areas and level of access, where required.

SERVICE DESK

- 2.11 The Service Desk will provide support to the Customer during the Support Hours. The Service Desk provides a single point of contact for all Customer enquiries, queries or Incidents logged by MyPortal, email or telephone.
- 2.12 When contacting the Service Desk the Customer must, where possible, provide details of the following:
 - 2.12.1 contract number;
 - 2.12.2 serial number or make and model;
 - 2.12.3 details of Supported Equipment;
 - 2.12.4 Customer contact information; and
 - 2.12.5 full description of the issue.

SUPPORT HOURS

- 2.13 From the Commencement Date, the Supplier shall provide the Service(s) in accordance with the Standard Support Hours, as further described below:

	DAYS	HOURS	BANK HOLIDAYS
Standard Support	Mon – Fri	09:00 to 17:30 Hrs	Excluded

INCIDENT IDENTIFICATION

- 2.14 The Customer shall report an Incident to the Service Desk as soon as reasonably practicable by telephone, email or MyPortal.
- 2.15 The Supplier shall identify and classify a request submitted to the Service Desk as either (i) an Incident or (ii) a Change Request as defined in **Annex 1**. All Incidents shall be managed in accordance with this paragraph 2.
- 2.16 Where a request is deemed by the Supplier to be a Change request, this Supplier may provide support subject to an Additional Charge calculated on a time and materials basis in accordance with the Supplier’s applicable Tariff from time to time.

INCIDENT MANAGEMENT

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

2.17 Where the Customer notifies the Supplier of an Incident in relation to the Supported Equipment or where a ticket is automatically generated or inputted by the Supplier, the Supplier shall log, process and manage Incidents through its Service Desk.

2.18 All Incident resolutions are verified with the Customer and/or its End Users in accordance with ITIL Methodology before the Incident is deemed Resolved.

2.19 For all Incidents relating to Excluded Events, equipment not listed as Supported Equipment or where the support requested or required is deemed outside of the scope of the Services, the Supplier shall use reasonable endeavours to respond to such Incidents, subject to an Additional Charge calculated on a time and materials basis in accordance with the Supplier’s applicable Tariff from time to time. Such Incidents shall not be counted or considered in relation to the performance of any Service Levels.

REMOTE SUPPORT

2.20 The Service Desk will aim to resolve Incidents at first line, where this is not possible, the Incident will be escalated to the appropriate 2nd / 3rd line subject matter expert in accordance with the Incident Management process.

2.21 Attendance at Site of an Engineer is not included within the Managed Security Support. If the Customer requests an Engineer to attend Site, this shall be subject to an Additional Charge calculated on a time and materials basis in accordance with the Supplier’s applicable Tariff from time to time.

PRIORITY CLASSIFICATION

2.22 The Supplier shall allocate a unique reference number to each Incident and shall prioritise the Incident as follows:

PRIORITY LEVEL	DESCRIPTION
Priority 1 Critical	A critical service is non-operational, impacting the Customer’s business, multiple End Users or multiple Sites; or severe functional error or degradation of Service(s) affecting production, demanding immediate attention. Business Risk is High
Priority 2 Major	The Customer’s business is experiencing failure or performance degradation that impairs the operation of a critical business Service, although a work around may exist; or Application functionality is lost; or significant number of End Users or major Site is affected. Business Risk is Medium
Priority 3 Minor	The Customer is experiencing a problem that causes moderate business impact. The impact is limited to an End User or a small Site; or incident has moderate, not widespread impact; or involves partial loss with minimal impact which is non-critical in nature. Business Risk is Low

Priority 6 Change Request	Standard service request (e.g. End User guidance and Change Requests); or updating documentation. Business Risk is Minor localised
-------------------------------------	--

2.23 Subject to paragraph 2.12 above, the Supplier shall use reasonable endeavours to deliver a Change Request as soon as reasonably practicable during Support Hours.

INVESTIGATION AND DIAGNOSIS

2.24 Tickets are manually inputted and processed by the Service Desk through MyPortal. Initial triage of the ticket, fact verification including incident prioritisation and classification are completed.

2.25 The Service Desk will then attempt to resolve or direct the Incident to the appropriate service team.

2.26 Throughout the Incident or Change Request, updates, notes and where appropriate log files and images will be placed on MyPortal. The status of an Incident or Change Request will change depending on the current actions required.

2.27 If an Incident or Change Request requires input from the Customer, the ticket will be placed in a deferred state until a response is received.

RESOLUTION AND CLOSURE

2.28 When the Incident has been Resolved, the notes, including a description of the resolution will be updated and made available for review by the Customer if required.

2.29 Where appropriate, communication will be made between all parties before the Incident is closed in accordance with Incident Management deliverables.

2.30 Incidents may also be closed, if after reasonable effort has been made to get a response from the Customer, no update has been given on three (3) consecutive occasions. In such cases Incidents can be reopened upon request by the Customer.

SERVICE LEVELS

2.31 The Supplier shall use its reasonable endeavours to ensure that response times to the Customer’s notification of an Incident are not more than:

PRIORITY LEVEL	CATEGORY	INITIAL RESPONSE TARGET* (NORMAL WORKING HOURS)
Priority 1	Critical	1 Hour
Priority 2	Major	4 Hours
Priority 3	Minor	8 Hours
Priority 6	Minor	5 Working Days

2.32 The initial response targets in paragraph 2.31 above are standard response targets. Where the Supplier has agreed specific response targets with a Customer, these shall be set out in the relevant Order.

**Calculated from receipt of notification of Incident by Supplier*

THIRD PARTY WARRANTY SUPPORT

2.33 Where the Supported Equipment has a valid Third-Party Supplier warranty and/or support contract in place, the Supplier shall facilitate on behalf of the Customer any claim made under the Third-Party Supplier warranty and/or

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

support contract, in respect of an Incident identified and logged with the Service Desk.

- 2.34 Where the Supported Equipment does not have a valid Third-Party Supplier warranty or support contract, or the Third Party Supplier no longer provides appropriate support, the Supplier shall use reasonable endeavours to respond to an Incident, subject to payment of Additional Charges or a sufficient balance of Resource Credits on the Customer account shown in MyPortal.

SYSTEM MONITORING

- 2.35 The Supplier shall provide real-time monitoring with intelligent alerting. For Endpoint solutions only, this is subject to the mandatory installation of the Supplier's preferred RRM Platform.
- 2.36 Subject to the Customer having the appropriate level of Managed Security Support as set forth in the relevant Order and the supported product being an endpoint solution, the Supported Equipment will be installed with RRM Agents to monitor and help manage the current state at any time, with data from the Supported Equipment being securely passed to the RRM Platform and displayed for the Supplier to action or escalate as appropriate.
- 2.37 The Supplier shall respond to SNMP and email alerts (both when mentioned in relevant annex only) and logon to the relevant console to inspect issues in accordance with the Service Level Targets.
- 2.38 A specification document detailing what the Supplier monitors and backs up can be provided to the Customer upon request.
- 2.39 In accordance with the Service Level Targets the Supplier will either attempt to resolve the issue on the Customer's behalf (only if the problem can be resolved from the relevant management console) or advise the Customer on what actions are required to take place to address the issue.

ELECTIVE CHANGE MANAGEMENT

- 2.40 The Supplier upon request by the Customer can undertake Change Requests and will manage all changes covered under the Services from scoping to release and testing in accordance with the Change Request process.
- 2.41 The Customer shall submit a Change Request through the Service Desk, subject to Additional Charges as follows:
- 2.41.1 Up to five (5) Elective Changes per month are included in the Service and shall be allocated for common changes that do not require a detailed scope of works; and
- 2.41.2 Customised Changes are specific to the Customer and are scoped on a case-by-case basis with the Customer being charged on a time and materials basis.
- 2.42 All additional Elective Changes are completed on a time/materials basis and charged to the Customer as per the Supplier's Standard Schedule of Rates.
- 2.43 The Customer may also purchase, at the Commencement Date, a specific quantity of Technical Attendance Days which will be set out in the applicable Order.
- 2.44 For the avoidance of doubt, Customised Changes under paragraph 2.41.2 above shall be outside of the scope and terms of this Schedule and subject to a separate Order, will be specified and carried out in accordance with **Schedule 4.2 (Professional Services)**.

SYSTEM BACK UPS AND DISASTER RECOVERY

- 2.45 The Supplier will take backups of the supported solution in accordance with the appropriate Annex.

- 2.46 In the event of a disaster, the Supplier will restore the Supported Equipment in accordance with the appropriate Annex.

- 2.47 This is limited to the Supported Equipment and the Supplier reserves the right to limit to one (1) restoration per Contract Year.

PATCH MANAGEMENT

- 2.48 Patching is only provided when an endpoint solution (with included anti-virus) is selected for inclusion in the support package.

- 2.49 It is the Customer's obligation to perform Device reboots on a regular basis and / or when notified by the patching solution or the Operating System. The Devices to be patched must also have an internet connection to the cloud hosted patching solution for correct policy enforcement. The Customer must also not alter with the deployed patching solution for the duration of Service.

- 2.50 The Supplier's remote patch management service ensures that all applicable patches/updates are being used. Hardware drivers, firmware and associated management Software are outside of the scope of the patch management.

- 2.51 The Supplier recommends that updates are applied to keep the Customer Network within the Third-Party Supplier's supported versions and the Customer can request the Supplier to undertake an infrastructure health check at any time during the Agreement, subject to an Additional Charge to the Customer.

- 2.52 The Customer is responsible for ensuring a current back up is in place and viable with respect to automatic patching and will report any failures to the Supplier so the affected patching schedules can be adjusted.

- 2.53 Emergency patches are subject to a Change Request and changes will be raised as and when either the Customer or the Supplier is made aware of the specific patch. The Customer may use the allocated Elective Changes included under paragraph 2.41 above, where the allocated number have already been used there will be an Additional Charge to the Customer.

- 2.54 In the event of an error, the Supplier shall remove or roll back the patch identified as causing the problem and snapshots may be used by the Supplier to facilitate the removal but only in instances deemed necessary by the Supplier. If the error is present on multiple devices, the Supplier has the right to remove or roll back the update on one device and provide guidance on doing this across the rest of the estate.

- 2.55 The Supplier shall support the following Operating Systems and Third-Party Supplier Software patching:

- 2.55.1 Microsoft Windows
- 2.55.2 Microsoft Office 365
- 2.55.3 7-Zip
- 2.55.4 Adobe AIR
- 2.55.5 Adobe Acrobat Reader DC
- 2.55.6 Google Chrome
- 2.55.7 Java Runtime Environment
- 2.55.8 Mozilla Firefox
- 2.55.9 Skype

within the current standard or extended support for patching of the applicable Third-Party Supplier. The Supplier reserves the

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

right to amend this paragraph and shall only support these products unless otherwise set forth on the relevant Order.

AUTOMATED REPORTING

2.56 The Supplier shall provide weekly automated reporting as defined in the applicable Annex.

ADVISORY SESSIONS

2.57 The Supplier shall provide as part of the Service, quarterly advisory sessions for up to one (1) hour with an Engineer, which will recap on any latest threats and to advise on any configuration adjustments that may be required.

2.58 The Supplier will advise on recommended rule and configuration changes and will implement upon agreement following the scheduled sessions either by using the Elective Change or Customised Change process.

3. CUSTOMER OBLIGATIONS

3.1 On and from the Commencement Date and for the duration of the Agreement, the Customer shall:

3.1.1 pay the Charges as and when they fall due;

3.1.2 make available all such facilities as the Supplier, and its Personnel reasonably require in providing the Security Support, including but not limited to:

(i) direct and remote access to the Customer Network, the Supported Equipment;

(ii) full and free access to the Site during the Support Hours; and

(iii) provide such reasonable assistance as the Supplier may request (e.g. providing sample output and other diagnostic information);

3.1.3 notify the Supplier immediately upon failure of any of the Supported Equipment;

3.1.4 ensure that the Supported Equipment is compliant with Applicable Law;

3.1.5 ensure that proper environmental conditions are maintained for the Supported Equipment and shall maintain in good condition the accommodation of the Supported Equipment, the cables and fittings associated therewith and the electricity supply thereto;

3.1.6 keep and operate the Customer Network and Supported Equipment in a proper and prudent manner, in accordance with the manufacturer's operating instructions, and ensure that only competent trained employees (or persons under their supervision) are allowed to access the Customer Network and Supported Equipment;

3.1.7 provide a secure, continuous power supply at the Site(s) for the operation of the Customer Network at such points with such connections as the Supplier specifies, and in order to mitigate any interruption to the Supported Equipment resulting from failure of the primary power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards;

3.1.8 ensure that all data held on the Customer Network is adequately backed up and keep full security copies of the Customer's programs, data bases and computer records and maintain a disaster recovery process;

3.1.9 be responsible for data cleaning, the integrity of any data provided to the Supplier and for all direct and indirect consequences of any errors in such data;

3.1.10 put in place and maintain up to date security measures to protect the Customer Network from viruses, harmful code, malicious damage and unauthorised direct and remote access to the Customer Network in accordance with Good Industry Practice;

3.1.11 procure and maintain all relevant licences and consents and, always comply with the terms of the relevant Supported Equipment and other licences and consents and all Applicable Law; and

3.1.12 inform the Supplier, in writing, of all health and safety rules and regulations and any other reasonable security requirements in place at the Customer Site(s), including any updates from time to time, and take all reasonable steps to protect the health and safety of the Supplier's Personnel whilst at the Customer's Site(s).

3.2 The Customer shall promptly implement recommendations by the Supplier in respect to remedial actions, whether prior to or following an Incident and confirms that it owns or will obtain valid Licenses for all Software which are necessary to grant the Supplier access to and use of the Software for the purpose of fulfilling its obligations under this Schedule.

3.3 The Customer shall inform the Supplier of any changes to its applications, underlying Operating System and/or maintenance and support on services not provided by the Supplier, which may affect the validity of the data to be obtained by the Supplier during an Audit.

3.4 The Supplier reserves the right, subject to providing the Customer with reasonable notice, to undertake an Audit of the Hardware and Software on an annual basis.

4. SERVICE CONDITIONS

4.1 The Supplier shall perform the Services;

4.1.1 using appropriately qualified and skilled personnel;

4.1.2 in accordance with this Schedule and the relevant level of Service;

4.1.3 with reasonable care and skill and in accordance with Good Industry Practice, and;

4.1.4 so as to conform with all statutory requirements and applicable regulations relating to the Services; and in accordance with the provisions of this Schedule as applicable and set forth in the applicable Order.

4.2 The Customer is required to provide accurate and up to date contact details for primary contact details that the Supplier can access as necessary, and it is the Customer's responsibility to keep the Supplier updated and provide secondary points of contact in case of absences. The Supplier shall not be responsible if a Service Failure occurs due to the Supplier not being able to contact the Customer.

SERVICE LIMITATIONS

4.3 The Supplier shall only provide the Services where the Customer meets the prerequisites as set out in paragraph 2 above.

4.4 Any work outside of the Services described in this Schedule shall be subject to an Additional Charge, this includes but is not limited to any Elective Charges exceeding 5 a month, any Customised Changes and all attendance at Site of an Engineer.

4.5 Configuration changes either requested or required as part of a resolution of an Incident or otherwise are not covered under Managed Security Support. These changes can be completed, subject to approval, and an Additional Charge

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

unless the configuration change is an Elective Change and is 1 of the 5 monthly allowance that is included as part of the Managed Security Support.

- 4.6 Upgrades to the Supported Equipment are not covered under Managed Security Support. Support with Upgrades can be provided, subject to approval and an Additional Charge.
- 4.7 The Supplier shall not be obliged to provide Services outside of Standard Support Hours or for any equipment other than the Supported Equipment. Equally, any requests not related to the security aspects of the solution will not be supported. Where support is provided, it is provided subject to an Additional Charge.
- 4.8 Managed Security Support does not include support directly on endpoints, support in relation to threat hunting or threat remediation. Where support is provided, it is provided subject to an Additional Charge.

5. CHARGES AND PAYMENT

- 5.1 The Supplier shall invoice the Customer for the Charges for the Services as set out in paragraph 5.2 in the amounts specified in the applicable Order or as varied pursuant to the terms of this Agreement.
- 5.2 Unless stated otherwise in the applicable Order or SOW, the Supplier shall invoice the Customer as follows:
 - 5.2.1 Installation Charges, on or after the Commencement Date;
 - 5.2.2 Recurring Charges annually in advance;
 - 5.2.3 Licence Fees annually in advance;
 - 5.2.4 Additional Charges monthly in arrears;
 - 5.2.5 any charges for Hardware, Devices and/or Software at the time of delivery of such Hardware, Devices and/or Software; and
 - 5.2.6 any Termination Charges upon termination of the Services.

hereinafter defined as “Charges”.

- 5.3 The Customer acknowledges and agrees that Licence Agreements can take up to sixty (60) days to be processed with the Third-Party Supplier.
- 5.4 Additional Charges shall be invoiced in arrears at the end of the month in which the Additional Charges are incurred, together with replacement parts and any other expenses and costs reasonably incurred.
- 5.5 The Supplier shall have the right to invoice Additional Charges to the Customer for any expenses and costs reasonably incurred under paragraph 6 below, or where the Supplier upon investigation an Incident is caused by something which the Supplier is not responsible for under this Schedule.
- 5.6 Unless otherwise stated in the Order, the Customer shall pay, by direct debit, each undisputed invoice (or such undisputed part thereof) within seven (7) days of the date of the invoice without any set-off or deduction.
- 5.7 Where the Customer in good faith disputes the Charges, the Customer shall notify the Supplier in writing within seven (7) days of the date of the invoice, in accordance with clause 6.17 of the General Conditions.
- 5.8 All Charges payable under this Schedule are exclusive of VAT which shall be paid by the Customer at the rate and in the manner prescribed by law.

- 5.9 If in the opinion of the Supplier, the Services are required by the Customer as a result of any misuse or neglect of, or accident to the Customer Network, and/or the Supported Equipment or due to the Customer not adhering to paragraph 3, or other third-party hardware problems, the Supplier reserves the right to charge an additional fee in relation to the provision of the Services.
- 5.10 The Supplier reserves the right to charge the Customer an Additional Charge for an Incident where the Supported Equipment has been moved to a new location and not installed by the Supplier, if the Supplier reasonably determined that the problem was caused by the transportation or re-installation of the Supported Equipment.
- 5.11 Where the Supplier finds that the Supported Equipment list does not contain all Software and/or Hardware forming the estate to which Services are being provided, the Supplier reserves the right to (i) vary the list to add such Software and/or Hardware; and (ii) increase the Recurring Charges in consideration for providing Services for the Supported Equipment added (“**Additional Supported Equipment**”). Where the Supplier exercises its right under this paragraph, the Customer shall be liable to pay the increased Recurring Charges in accordance with this clause 5 and the General Conditions.

6. EXCLUSIONS

- 6.1 Notwithstanding any other provision of this Schedule or the General Conditions, the Supplier shall not be obliged to perform or provide the Services in one or more of the following circumstances:
 - 6.1.1 the Customer is in breach of its obligations under paragraph 3 above or is in material breach of this Agreement;
 - 6.1.2 negligence of the Customer or its End Users or the improper use by the Customer or its End Users of the Customer Network and/or Supported Equipment;
 - 6.1.3 damage to the Supported Equipment resulting from accident, transportation or relocation, neglect, misuse or causes other than ordinary use (including but not limited to, failure to observe any instructions supplied by the manufacturer regarding the operation and maintenance) of the Supported Equipment;
 - 6.1.4 damage caused by consumable items such as recording materials, machine stationary, ribbons, media, laser drum, toner, printer cartridges, paper trays, platen knobs, fuses, batteries, print heads, cathode ray tubes, switch boxes, power adaptor blocks or any other item considered to be a consumable by the Supplier;
 - 6.1.5 damage caused by the use of non-manufacturer approved consumables, where this results in abnormal wear or damage to the Supported Equipment;
 - 6.1.6 damage caused by virus attacks or failure due to any unauthorised third party Software;
 - 6.1.7 alteration, modification, repair or maintenance of the Supported Equipment by any person other than the Supplier or its approved Third Party Supplier;
 - 6.1.8 the Supported Equipment is removed from Site without the prior written approval of the Supplier;
 - 6.1.9 insufficient or improper access to the Customer Network and/or Supported Equipment;

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

- 6.1.10 failure or fluctuations in electrical power supply and/or unsatisfactory environmental conditions which do not meet manufacturers requirements;
 - 6.1.11 where the Customer's own insurance covers the accidental or malicious damage to the Supported Equipment and costs relating to the Supported Equipment; and
 - 6.1.12 damage to the Customer Network and/or Supported Equipment due to accidental damage, theft, vandalism or a Force Majeure Event.
- 6.2 Where the Supplier is called out in connection with any of the matters referred to in paragraph 6.1 or where the Supplier determines that the call was not warranted, the Supplier has the right to charge the Customer for any expenses and costs reasonably incurred as Additional Charges.
- 6.3 For the avoidance of doubt, the excluded events as listed in paragraph 6.1 above shall not be counted or considered in relation to the performance of any Service Levels.

7. LIABILITY

- 7.1 This paragraph 7 is supplemental to clause 9 of the General Conditions and the event there is an express conflict with clause 9 of the General Conditions this paragraph shall take precedence.
- 7.2 The Customer shall indemnify the Supplier and keep the Supplier fully and effectively indemnified in full on demand against all costs, charges, damages and or any losses sustained or incurred by it arising directly or indirectly from the Customer's failure to perform or delay in the performance of its obligations under this Schedule or from any fraudulent or negligent act or omission or wilful misconduct of the Customer, its End Users, employees, agents or subcontractors.
- 7.3 The Supplier shall not be liable to the Customer for any loss arising out of any failure by the Customer to keep full and up to date security copies of the computer programs and data it uses in accordance with Good Industry Practice.
- 7.4 The Supplier shall not be liable for failing to perform the Services or delaying the Services hereunder by reasons of Force Majeure. If a Force Majeure event prevents the Supplier from providing the Services for more than three (3) months, the Supplier shall, without limiting its other rights and remedies, have the right to terminate this Schedule in relation to any affected Services immediately by giving written notice to the Customer.

8. TERMINATION

- 8.1 This paragraph 8 is supplemental to clause 8 of the General Conditions and in the event this paragraph 8 conflicts with clause 8 of the General Conditions, this paragraph shall take precedence.
- 8.2 The Customer may terminate the Services generally or in relation to any part of the Services at any time by giving the Supplier not less than ninety (90) days written notice prior to the end of the Minimum Term or Successive Term, such notice to take affect at the end of the Minimum Term or Successive Term.
- 8.3 The termination of one or more element of the Services shall not affect the continuing in effect of the remaining Services, including but not limited to the Supplier's obligation to perform the remaining Services and the Customer's

obligation to perform its responsibilities and make payment of the Charges in accordance with this Schedule.

- 8.4 In the event of a termination pursuant to paragraph 8.1.1 of the General Conditions, the Customer shall not be entitled to reimbursement of any aspect of the Charges as shall have been paid in advance and relate to the Services.

9. GENERAL

- 9.1 The Customer shall not, without the prior written consent of the Supplier, at any time during the Minimum Term of this Schedule nor for a period of six (6) months following its expiry or termination for any reason, solicit or entice away from the Supplier or employ any person who is, or has been, engaged as an employee of the Supplier at any time during such period. Any consent given by the Supplier shall be subject to the Customer paying the Supplier a sum equivalent to one hundred per cent (100%) of the then current annual remuneration of the Supplier's employee.
- 9.2 The Customer acknowledges and agrees that TUPE shall not apply to the Services and prior to the Commencement Date, all considerations, claims, actions or otherwise have been provided to the Supplier in relation to the effects, actions or claims of any TUPE and that the Customer indemnifies in full and holds the Supplier harmless of any such actions or claims of TUPE against the Supplier for business transfers or service provision changes for the Term of this Schedule and for a period of six (6) months following expiry or termination of this Schedule.

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

ANNEX 1 – DEFINITIONS

Additional Charges means the additional charges incurred in accordance with terms of this Schedule together with any replacement parts and any other costs or expenses reasonably incurred if not expressly included in the relevant Order;

Applicable Law means any legislation, authorisations, permissions, rules and regulations, codes of practice, orders and guidelines relating to the provision of the Infrastructure Support Services, including any directives or other requirements issued by any regulator from time to time;

Applications means a computer software package that performs a specific function directly for and End User or, in some cases, for another application, also referred to as an application program or application software;

Change Request means a formal request to change, modify or alter the Services provided by the Supplier to the Customer as set forth in the applicable Order;

Charges has the meaning given to it in paragraph 5.2;

Contract Year means a period of twelve (12) months from the Commencement Date and/or any subsequent anniversary of the Commencement Date;

Customer Equipment means any equipment including purchased Hardware, Devices and Software used by the Customer in connection with the provision of the Services;

Customer Network means the Customer's physical network and server infrastructure, including (if any) servers and switches to routers and firewalls, plus business systems software;

Device means any mobile handset, laptop, tablet, computer or other input item or handheld equipment, including all peripherals, excluding SIM cards and Applications, which are in the scope of the Services, as set out in the Order;

End User means anyone permitted by the Customer to use or access the Supported Equipment, Customer Network and/or the Customer Equipment;

Engineer means the Supplier's Personnel who is responsible for carrying out technical engineering duties either remotely or at a Customer's Site;

Excluded Events means the events and circumstances listed at paragraph 6.1

Force Majeure shall have the meaning given to it in Clause 9.6 of the General Conditions;

General Conditions means the Supplier's standard terms and conditions for the provision of the Services as set forth on the Supplier's website at www.chessict.co.uk/legal and which form part of this Agreement;

Good Industry Practice means in relation to any undertaking and any circumstances, the exercise of that degree of skill and care which could be reasonably expected of a highly skilled and experienced professional;

Hardware means any and all computer and computer related hardware, including but not limited to, computers, servers, network switches, UPS units, firewalls and connect peripherals;

Incident means any event which is not part of the standard operation of the Supported Equipment and which causes or

may cause an unplanned interruption to, or a reduction in the quality of the performance of the Supported Equipment;

Incident Management is the process as further defined in paragraph 2 of this Schedule;

ITIL Methodology means a set of IT Service Management practices that focuses on aligning IT services with the needs of business;

Installation Charges means the charges in relation to the installation of the Supported Equipment, Services or any Customer Equipment as applicable;

Licence Agreement(s) means any licence or terms under which the Customer is permitted to use third party Software;

Licence Fees means the charges associated with the use of the Software, by the purchase of a Licence Agreement;

MyPortal means the Customer's online access to the provision of the Services available through the Supplier's website at <https://chessict.co.uk>;

Operating System means system software that manages computer hardware, software resources, and provides common services for computer programs;

Order means an order issued by the Supplier to the Customer for the provision of the Services;

Professional Services means engineering support as further detailed in **Schedule 4.2 (Professional and Consultancy Services)**;

Recurring Charges means the Charges for the Managed Security Support which are invoiced repeatedly in every billing period as set out in the Order;

Resolved or Resolution means where an Incident has been resolved and the standard operation of the Customer Network and/or Supported Equipment as is expected in accordance with manufacturers recommendations;

Services means Managed Security Support;

Service Desk means the Supplier's Service Desk that the Customer is able to contact to report an Incident;

Service Levels means the relevant Service Level targets as further defined in paragraph 2 of this Schedule;

Site(s) means the Customer's premises at which the Customer Network and/or Supported Equipment is located as specified in the relevant Order;

Software means the software licensed to the Customer, together with any embedded software which is necessary for provision of the Services and/or operation of the Supported Equipment, which may be provided by a Third-Party Supplier and governed by a separate Licence Agreement;

Standard Support Hours means 09:00hrs to 17:30hrs on a Working Day;

Supplier's Personnel means all employees, agents, consultants, sub-contractors and other representatives of the Supplier who are involved, or proposed to be involved, in the provision of the Services;

Supported Equipment means the list of Hardware and/or Software as further detailed in the relevant Order or SOW and for which the Service is being provided in accordance with this Schedule;

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

Technical Attendance Days means where an Engineer attends Site to carry out Elective Changes during Standard Support Hours, excluding consumables and spare parts;

Termination Charges mean any compensatory charges payable by the Customer to the Supplier upon termination of this Agreement, in whole or part, in accordance with clause 8.7 of the General Conditions and as set out in the applicable Order, or if not specified then an amount equal to 100% of the Recurring Charges for all remaining months for the Minimum Term, together with any waived one off charges or Installation Charges;

Third Party Supplier means a third-party supplier, provider or supplier of services of which:

- (a) the Customer may utilise for the provision of equipment and the Customer's Network, and;
- (b) the Supplier may utilise for provision of the Services;

TUPE means the Transfer of Undertakings (Protection of Employment) Regulations 2006;

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

ANNEX 2 – SOPHOS

- Where the Supported Equipment includes Sophos Software and/or Hardware this **Annex 2** applies and take precedence over the Schedule in the event of express conflict.

Initial Configuration

- The Customer shall provide suitable alternative servers and infrastructure and must ensure that they meet the Sophos Endpoint and XG minimum requirements which can be found at <https://docs.sophos.com/>.
- Sophos currently offers Central installers for the following end points:
 - Windows 7 desktop and above
 - Windows Server 2008 R2 and above
 - MacOS 10.15 and above;
 - Linux 10 (as per Sophos KB Sophos Anti-Virus for Linux: system requirements)

Installation can take up to 10 minutes to complete once downloaded.

- If the existing AV software is not removable by the Sophos CRT tool then additional work will be required by the Supplier to investigate, test and perform the removal process, which would be chargeable to the Customer at the Supplier’s standard rates applicable at the time. The current Sophos CRT tool third party AV compatibility list is available from the following link https://support.sophos.com/support/s/article/KB-000034009?language=en_US.
- The standard Software installation and configuration options and the pre-requisites are shown below;

	INSTALLATION OPTIONS	PRE-REQUISITES
Unmanaged Network with no AV	Locally run the installer on each End Point Email a link to End User to self-install	Internet Access Local Admin privileges on End Point
Unmanaged Network with current AV solution	Locally run the installer on each End Point Email a link to End User to self-install	As above Existing AV product must be compatible with Sophos CRT tool
Managed Network with no AV	Locally run the installer on each End Point Email a link to End User to self-install Remotely deploy a script	Internet Access Local Admin privileges on End Point Customer to provide support for management tools

Managed Network with Managed AV	As above	As above Existing AV product must be compatible with Sophos CRT tool
--	----------	---

- Where the Customer’s internet access for End Points is restricted for security reasons or internet connectivity is very poor, a local cache/message relay server can be deployed, however this will require additional time to enable the Supplier to configure and test.
- If the Operating Systems are not supported by the manufacturer but are supported by Sophos, and an extended subscription has been purchased, if required and the Supplier shall use reasonable endeavours to support the same.
- The Customer is responsible for ensuring it has the appropriate Sophos License Agreements in place for the infrastructure environment and each End User and acknowledges that provision of Managed Security Support is dependent upon such License Agreements being in place at the point of implementation and for the duration of the Agreement.
- Where the Customer purchases Sophos products through the Supplier, the terms of **Schedule 3.6(B) Sophos Endpoint and Security Protection Products** apply and as detailed therein the Customer also accepts the applicable Sophos End User terms and conditions.
System Monitoring
- SNMP alerts only available with the XG firewall solution. Email alerts are available on both Sophos Central and Sophos XG.
System Backups and Disaster Recovery
- The Supplier will take backups of the XG firewall (Configuration not reporting data) when this service option has been selected. This configuration will be stored on the Supplier’s servers
- In the event of a disaster, the Supplier will restore the Supported Equipment/Sophos XG Firewall using remote access and the Customer is required to have on Site assistance during such time to support the Supplier remotely. The Supplier is not responsible for restoring clients and servers either from a disaster or due to a failed patch.
Automated Reporting
- The Supplier shall provide automated reporting that will include an overview of the following:
Sophos Central
Threats
 - Malware Detected
 - Total websites warned
 - Total websites blocked
 - Exploits Prevented
 System Health
 - Total computers protected
 - Total servers protected
 - Total users protected
 - Most frequently blocked applications

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

XG Firewalls

Threats (Web/Email/IPS/ATP)

- Security Audit Report
- Executive Report

Upgrades

14. Where the Supported Equipment is an XG Firewall point upgrades are included as part of Managed Security Support and are not subject to an Additional Charge in accordance with paragraph 4.6 of the Schedule.

ANNEX 3 – MICROSOFT

1. Where the Supported Equipment includes Microsoft Software and/or Hardware this **Annex 3** applies and takes precedence over the Schedule in the event of express conflict.

Initial Configuration

2. Microsoft's minimum requirements can be found at <https://www.microsoft.com/en-gb/microsoft-365/microsoft-365-and-office-resources>.
3. For endpoints, professional versions of Windows 10 and 11 are required.
4. Microsoft Managed Security Support for a supported server OS includes a Microsoft Defender for Endpoint license.
5. If the existing AV software does not have a central removal tool, then additional work will be required by the Supplier to investigate, test and perform the removal process. The Supplier shall be entitled to invoice the Customer Additional Charges calculated on a time and materials basis and in accordance with its Tariffs applicable from time to time. The current non - Microsoft removal tool is available from the following link <https://support.microsoft.com/en-us/topic/list-of-security-program-cleanup-and-uninstall-tools-751fd6cc-a39f-dc66-ef44-61a7de91b7dc>
6. Subject to the Customer having in place the relevant License Agreements with Microsoft, the Supplier will implement the Microsoft security related features referred to in paragraph 9 of this Annex 3 in accordance with industry best practice. To do so the Customer must provide to the Supplier:
 - Global administrator permission, or delegated permission's equivalent role, to the Customer's active Microsoft 365 Tenancy through for the duration of the Agreement; and
 - Provide any existing computer and bring your own device policies in place with the Customer's organisation and (i) accept any required changes to such policies to support the secure configuration of the components listed in paragraph 2.2 of the Schedule; or (ii) create a policy that supports the security configuration and implement that policy within the Customer's organisation, and if required the Supplier can provide a basic policy.
7. The Supplier will provide the following configuration:
 - Configuration of policies to facilitate End User device management;
 - Configuration of Endpoint security policies;
 - Configuration of Office 365 security policies;

- Configuration of Azure Active Directory security policies including conditional access;
- Configuration of Data Protection for Microsoft 365; and
- Configuration of relevant role-based access controls to prevent alteration of required security policies.

8. Further information in relation to the configuration referred to above, is detailed in the Supplier's proposal document.

Service Description

9. In addition to what is stated in paragraph 2.2 of the Schedule, the Supplier will also provide the customer with the following:
 - Device management utilising Microsoft Intune and Endpoint Manager
 - Endpoint protection utilising Microsoft Defender
 - Cloud Protection utilising Defender for Office 365
 - Identity protection utilising Azure Active Directory
 - Cloud back-up utilising Data Protection for Microsoft 365.
 10. The Customer is responsible for ensuring it has the appropriate Microsoft License Agreements in place for the infrastructure environment and each End User and acknowledges that provision of Managed Security Support is dependent upon such License Agreements being in place at the point of implementation and for the duration of the Agreement.
 11. Where the Customer purchases Microsoft products through the Supplier, the terms of **Schedule 3.6(A) Microsoft Services** apply and as detailed therein the Customer also accepts the applicable Microsoft End User terms and conditions.
 12. The Supplier will provide the Customer with Licenses for the Data Protection for Microsoft 365 referred to in paragraph 2.2.8 for use with the Managed Security Support as described in this Schedule. Except where provided for otherwise in this Schedule, **Schedule 3.9 Data Protection for Microsoft 365** shall apply to the provision of such Licenses.
- ### **System Monitoring**
13. Pro-active monitoring is currently not available and as such paragraphs 2.35 to 2.39 of the Schedule are not applicable where the Supported Equipment is Microsoft Software or Hardware.
- ### **Systems Back Up and Disaster Recovery**
14. The Supplier will take regular back-ups of the Customer's Microsoft 365 data in accordance with the Supplier's standard back-up schedule unless a specific back-up schedule is agreed with the Customer upon implementation. The Supplier will perform on demand restoration of the same in the event of a disaster in accordance with **Schedule 3.9 Data Protection for Microsoft 365**.

SCHEDULE 4.6(B) – MANAGED SECURITY SUPPORT

15. The Supplier will restore the Customer's Microsoft 365 data using remote access. The Customer is required to have on Site assistance during such time to support the Supplier remotely. The Supplier is not responsible for restoring clients and servers either from a disaster or due to a failed patch.

Automated Reporting

16. The Supplier shall provide automated reporting that will include an overview of the following:

Cloud (Office 365):

- Malware detected in email
- Phishing emails
- Spoof detection
- Spam Detections
- Compromised Users

17. The Customer acknowledges that that Microsoft will continue to develop and amend the various components listed above and as such any reporting functionality may be subject to change due to changes to the components comprised within the Microsoft License.