SCHEDULE 4.6 (C) – SOPHOS MANAGED SECURITY SERVICES

1. APPLICATION

1.1 This Schedule, which contains a description of the **Managed Security Services**, forms part of the Agreement between the Parties for the provision of Services together with the **General Conditions**.

1.2 Definitions and interpretations 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 The provision of Managed Security Services is subject to the Customer having deployed the required Products. Where the Customer purchases Products from the Supplier provision of the same shall be governed by the terms of **Schedule 3.6 (B) Sophos Endpoint and Security Protection**.

1.4 Where the Customer purchases Professional Services to support deployment of the Products, the provision of such service shall be governed by the terms of **Schedule 4.2 Professional Services**.

1.5 Where the Customer purchases Security Support Services relating to the Products from the Supplier, the provision of such service shall be governed by the terms of **Schedule 4.6(A) Standard Security Support** and **Schedule 4.6(B) Managed Security Support** as applicable.

2. SERVICES

2.1 The Supplier shall provide the Customer with managed security services, comprising of one or more of the following, where stated on the Order, and subject to the terms of this Agreement and the **End User Terms**;

2.1.1 Managed Detection and Response ("**MDR**");

2.1.2 Managed Detection and Response Complete ("**MDR Complete**");

2.1.3 Rapid Response; and/or

2.1.4 Threat Adviser.

Hereinafter defined as "**Managed Security Services**".

2.2 Notwithstanding anything to the contrary in this Schedule, the Customer acknowledges and agrees that: (i) Sophos may modify or update the Managed Security Services from time to time without materially reducing or degrading its overall functionality; and (ii) the Supplier may modify or update this Schedule at any time to accurately reflect the Services by giving notice in accordance with clause 16.1 of the **General Conditions**.

2.3 The Supplier is a Sophos MSP and Reseller and is authorised to distribute and re-sell the Managed Security Services.

3. COMMENCMENT AND DURATION

3.1 This paragraph 3 shall supersede clause 2.1 of the **General Conditions**. Managed Security Services can be purchased on an **Advanced Subscription** or **Pay-Monthly Subscription** basis, save for Sophos Threat Adviser which is only available on an Advanced Subscription basis.

3.2 Where the Customer purchases an **Advanced Subscription**, this Agreement shall become effective on the date of the **Order**. It shall continue for the minimum period stated on the **Order** from the Commencement Date ("**Minimum Term**") unless terminated in accordance with clause 8 of the **General Conditions**. Upon expiry of the Minimum Term, both the Agreement and Subscription automatically expire and do not renew.

3.3 Where the Customer purchases **a Pay Monthly Subscription**, this Agreement shall become effective on the date of the **Order**. It shall continue for the minimum period stated on the **Order** from the Commencement Date ("**Minimum Term**"), and thereafter unless terminated:

3.3.1 by the Customer giving the Supplier no more than 90 days' and not less than 30 days' written notice; or

3.3.2 in accordance with clause 8 of the **General Conditions**.

4. MDR SERVICE DESCRIPTION

4.1 Sophos Intercept X Advanced with XDR is referred to as "**Sophos XDR**" and Sophos XDR Sensor is referred to as "**XDR Sensor**". Where Service Software is used with reference to MDR or MDR Complete, it shall mean Sophos XDR or XDR Sensor as applicable.

4.2 **Onboarding**. During the onboarding process, the following activities must be performed by the Customer as a precondition to delivery of the Service:

4.2.1 provide contact information;

4.2.2 confirm communication preferences;

4.2.3 determine the Threat Response Mode;

4.2.4 install the required Service Software on all Managed Endpoints to be covered by the Service; and

4.2.5 configuration of any Third-Party Systems.

4.3 The Threat Response Modes available to the customer determine the interaction between the Customer and Security Service Team when an Investigation requires a Threat Response are:

4.3.1 Collaborate: The Security Service Team will conduct Investigations but no Response Actions are taken without the Customer's prior consent or active involvement. Certain actions such as remote query may be undertaken without Customer consent or involvement; or

4.3.2 Authorize: The Security Services Team performs Threat Response independent of the Customer and the Customer is notified of the Response Actions taken.

4.4 An option exists under the Collaborate Threat Response Mode which, if selected, authorises the Security Services Team to operate in Authorize mode in the event Sophos does not receive response from the Customer after contacting the Customer's named contacts.

4.5 **Sophos Account Health Check.** Health Check capabilities are only available on Managed Endpoints running Sophos XDR. A Health Check will be undertaken on all Managed Endpoints as part of the Onboarding Process.

4.6 The Customer will be notified of any configuration changes that could diminish the Customer's security posture along with the required steps to remediate the issues identified by the Health Check. Failure by the Customer to implement recommendations may result in diminished Service quality.

4.7 **Triage, Investigation and Threat Response**. Sophos will conduct the following investigation and analysis activities for Cases originating from Managed Endpoints:

4.7.1 analysis is conducted to enhance identification, aggregation, and prioritization of Detections, resulting in machine-generated Cases;

4.7.2 investigations are performed to confirm threats, and Threat Response is performed where appropriate. During Service performance, the Security Services Team

may use the results of Investigations to filter out expected activity to enhance visibility of suspicious activities in the Customer's environment; and

4.7.3 notification and information about the Case is shared with the Customer based on the Customer's pre-selected communication preferences.

4.8 **Availability.** All monitoring, investigation, and Response Actions described in paragraph 4.7 will be provided on a 24/7/365 basis. The Customer shall also have direct call-in access to the Security Services Team to review suspected incidents on a 24/7/365 basis.

4.9 **Service Level Targets.** The following service level targets apply to Investigations on Managed Endpoints and Third-Party Systems and provide guidelines around timing expectations for Case creation and Response Actions resulting from Investigations but excluding Threat Hunting.

Target time for Case creation	2 minutes from Detection
Target time for initial Response Action	30 minutes from Case creation

4.10 **Threat Hunting**. The Security Service Team will conduct Threat Hunting to proactively search for threats that may have evaded existing detection controls based on threat intelligence and Investigations. Threat Hunting is limited to data collected from Managed Endpoints and supported Third-Party Systems and will focus on identification of attacker's behaviours and tactics. If Threat Hunting reveals indicators of malicious activity, a Case will be created, and an Investigation will be performed.

4.11 **Threat Response.** Threat Response includes threat containment and disruption and endpoint isolation on Managed Endpoints, and where possible, may provide Third-Party Remediation Guidance.

4.12 **Reporting**; **Health Monitoring; Notification**. Periodically, the Customer will be provided with: (a) reports relating to Detections, Cases, and Response Actions; and (b) notification of Health issues or significant misconfigurations that can degrade real-time protection, investigation, or the ability to take Response Actions.

4.13 **Remote Access Tools.** To support Service delivery, the Security Services Team may use Sophos owned or selected remote access tools to access or make changes to Managed Endpoints and may utilize administrative access to Customer's Sophos Central environment to view or modify configurations.

4.14 If the Customer has selected Authorize Response Mode access will not require additional approval from the Customer. If the Customer has selected Collaborate Response Mode then Sophos will request necessary authorisation before performing any modifications. All access by the Security Services Team is logged and recorded.

4.15 THE CUSTOMER ACKNOWLEDGES AND AGREES THAT ITS AUTHORIZATION FOR SOPHOS TO MAKE ANY CHANGES TO, OR MODIFY CONFIGURATIONS IN, CUSTOMER'S ENVIRONMENT COULD RESULT IN INTERRUPTION OR DEGRADATION OF CUSTOMER'S SYSTEMS AND INFRASTRUCTURE.

4.16 THE CUSTOMER FURTHER ACKNOWLEDGES THAT FAILURE TO GRANT AUTHORISATION FOR SUCH CHANGES COULD RESULT IN NEW MALICIOUS ACTIVITY OR THE WORSENING OF EXISTING MALICIOUS ACTIVITY IF THE CUSTOMER HAS DENIED SOPHOS' REQUEST FOR AUTHORISATION TO MAKE CHANGES OR MODIFICATIONS.

5. MDR COMPLETE SERVICE DESCRIPTION

5.1 MDR Complete includes MDR as detailed at paragraph 4, together with the following:

5.1.1 **Remote Incident Response** is available in the event of a security incident on Managed Endpoints running Sophos XDR prior to the occurrence of the Incident. It includes the following activities:

5.1.1.1 assignment of a dedicated Incident Response Lead (one per shift) to interface with the Customer;

5.1.1.2 perform triage and Investigation to identify the scope and impact of the Incident to support containment;

5.1.1.3 analysis of additional data sources and data provided or made available by the Customer;

5.1.1.4 Response Actions will be taken to neutralise malicious access and stop further damage to compromised assets or data;

5.1.1.5 provide remediation guidance where the Security Services Team is unable to perform Response Actions and requires Customer involvement;

5.1.1.6 Incident status reporting and action item tracking; and

5.1.1.7 proactive recommendations designed to prevent or reduce reoccurrence of the Incident.

5.1.2 **Direct Call-In Access** to Security Service Team to review Cases and Incidents;

5.1.3 **Investigation** of Cases originating from the other MDR Compatible Sophos Products for which the Customer has a License;

5.1.4 **Service Legal Agreement** as detailed in this paragraph 5; and

5.1.5 where the Customer has purchased an MDR Complete Advanced Subscription, the **Breach Protection Warranty** provided by Sophos in accordance with Sophos' terms available at https://www.sophos.com/en-us/legal/mdr-complete-warranty.

SERVICE LEVELS

5.2 The SLA refers to Response Times by the Security Services Team for Customers who have purchased the MDR Complete Subscription. Customers who had a Sophos Managed Threat Response Subscription and were migrated to MDR Complete will not be entitled to the SLA's until such Customers renew their MDR Complete Subscription.

5.3 The following definitions apply to the SLA's:

5.3.1 "**High Severity Case**" means a Case created from Detections generated automatically by policies or analytics applied to telemetry from Managed Endpoints and/or Third-Party Systems that is determined to be of high or critical severity after review by the Security Services Team; and

5.3.2 "**Response Time**" means the elapsed time between the identification of a High Severity Case and the time the Security Services Team initiates: (i) contact to notify Customer of such High Severity Case either via email or phone, or (ii) Response Action for Customers that have been selected "Authorize" Threat Response Mode.

5.4 **Service Commitments.** Response Time will be within 60 minutes for 90% of High Severity Cases measured monthly beginning on: (i) the first day of the Service subscription renewal date for Existing Customers; and (ii) the first day of the fourth month of Sophos' provision of the Service for the new Customers. If Sophos misses the foregoing Response Time more than 3 times in any rolling 12-month period, then Sophos shall be deemed to have missed the SLA.

5.5 Where the SLA has been missed as described above, the Customer will be entitled to a credit equal to 5% of the Charges paid by the Customer for MDR Complete in the previous billing period or £5,000 whichever is lower ("**Service Credit**").

5.6 The Customer must request a Service Credit by email to SLACreditClaims@sophos.com with "*MDR Service Credit*" in the subject within 30 days from the date the Customer becomes eligible to receive a Service Credit and must be supported by evidence from log or report data. If not requested within the 30-day period, the Service Credit will expire and no longer claimable. The Customer will be entitled to claim a Service Credit no more than 3 times in any calendar year. All Service Credits will be subject to verification by Sophos.

5.7 **Exclusions**. Sophos will not be responsible for meeting the SLA in whole or in part due to conditions provided in paragraph 7 below.

6. MDR AND MDR COMPLETE CUSTOMER RESPONSIBILITIES

6.1 The Customer acknowledges and agrees it must take the following actions to facilitate and enable delivery of the Service, and the Supplier and Sophos shall have no liability for any degraded, incomplete or failed Service delivery which may result from Customer's failure to take required actions:

6.1.1 **Onboarding**. The Customer will perform all required activities during the Onboarding process;

6.1.2 **Installation Requirements.** The Customer must have:

6.1.2.1 a valid, active Sophos Central account;

6.1.2.2 deploy and configure the applicable Service to Managed Endpoints;

6.1.2.3 maintain compliance with all Health Checks;

6.1.2.4 meet minimum system requirements to install Service Software;

6.1.2.5 set up an configuration of all Third-Party Systems to enable transmission of all applicable security telemetry to Sophos in a format that is compatible with the Service; and

6.1.2.6 run only supported versions of the Service Software and/or third-party security tools;

6.1.3 **Remediating Known Threats.** The Customer must make reasonable efforts to timely remediate any compromises reported by the Supplier, Sophos or third-party technologies that the Customer utilises for cybersecurity detection and protection. Sophos and the Supplier shall not be responsible or liable for any issues caused by the Customer's failure to take remediation steps in a timely manner. The Security Services Team shall have no obligation to notify the Customer or generate new Cases from Detections for which Sophos has already recommended remedial steps;

6.1.4 **Time and Date Settings.** The Customer must ensure that all Managed Endpoints have accurate time and date settings. Sophos and the Supplier shall not be responsible for errors, issues and residual risk experienced or incurred by the Customer for Detections generated by Managed Endpoints with inaccurate time and date settings;

6.1.5 **Customer Personnel.** The Customer must identify an appropriate number of suitably skilled personnel who will work with the Supplier and Sophos during the provision of Services. The Customer's personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service;

6.1.6 **Timely Response.** The Customer must promptly acknowledge receipt of Sophos communications in writing (via email or other agreed method) and must timely respond to the Suppliers and Sophos' requests.

6.1.7 **Actions Outside the Scope of Service.** All activities that are not expressly provided for in this Schedule are outside of the scope. The Customer is solely responsible and liable for:

6.1.7.1 neutralizing any Incidents and/or confirmed threats in Third-Party Systems that cannot be resolved by Sophos;

6.1.7.2 taking any actions that are outside the scope of the Service e.g., Sophos suggested on-site response, e-discovery and litigation and collaboration with law enforcement;

6.1.7.3 for any actions undertaken by the Supplier or Sophos that are not provided in this Schedule but which are under the Customer's specific direction; and

6.1.7.4 any security incidents, threats or compromises that occurred or existed prior to the Commencement Date of the Service.

6.1.8 **Non-Sophos Systems.** The Customer acknowledges that Sophos and the Supplier:

6.1.8.1 are not responsible for any changes made to any non-Sophos systems by their vendors or any party that impact either the integration with Service or Sophos' ability to the provide the Service;

6.1.8.2 may, at their discretion, add, remove, and modify supported non-Sophos systems and it is the Customer's responsibility to check the supported list;

6.1.8.3 are not responsible for any Third-Party Systems integrations function and continue to function properly throughout the duration of the Agreement; and

6.1.8.4 if Third-Party Systems have not been properly configured or do not support transmission of security telemetry to Sophos, in which case, Sophos will reasonably work with the Customer to enable security telemetry transmission.

6.2 The Customer acknowledges and agrees that Service Software must be deployed on 80% of licensed volume as this is necessary to provide Security Services Team with sufficient visibility into Customer's environment for Service delivery.

6.3 The Supplier and Sophos reserve the right to suspend Service delivery until such time as the Customer performs the required actions. Failure to complete the required after written notice from the Supplier or Sophos (including email notice from the Security Services Team to Customer designated contacts) shall constitute material breach by the Customer of the Agreement.

7. MDR AND MDR COMPLETE EXCLUSIONS

7.1 **Service Exclusion.** The Customer agrees and acknowledges that the Supplier and Sophos will not be liable or be considered in breach of the Agreement (including the SLA's):

7.1.1 due to any delay or failure to perform its obligations hereunder as a result of industry or infrastructure wide ransomware, cyberwarfare or other cyberattacks that causes the Security Services Team to be unable to provide resources to address an Incident in a timely manner;

7.1.2 due to unforeseen circumstances or causes beyond Sophos reasonable control including but not limited to war, strike, riot, crime acts of God, or shortages of resources;

7.1.3 due to legal prohibition, including but not limited to passing of statute, decree, regulation, or order;

7.1.4 during any period of Service suspension in accordance with the terms of the Agreement;

7.1.5 if the Customer is in breach of this Agreement (including without limitation if Customer has any overdue invoices); or

7.1.6 during any scheduled maintenance window.

7.2 The Customer agrees and acknowledges that while Sophos has implemented commercially reasonable technologies and process as part of the Service, Sophos makes no guarantee that the Service will detect prevent, or mitigate all Incidents. The Customer agrees not to present to any other person or party that Sophos or the Supplier have provided such a guarantee or warranty.

8. RAPID RESPONSE SERVICE DESCRIPTION

8.1 The Rapid Response Service combines MDR Complete with Threat Response during an Incident present at the point the Customer placed an Order for the Service. All aspects of the Service will be provided remotely.

8.2 Rapid Response includes the scope and benefits of MDR Complete support services as detailed above at paragraphs 5.1.1 to 5.1.3 in relation to the Incident present at the point of Order in addition to the following:

THREAT NEUTRALISATION PROCESS

8.2.1 **Kick Off.** A kick-off call will be conducted to: a) exchange information about the Incident and Customer's existing infrastructure; b) identify the scope and impact of the Incident; c) mutually define a response plan; d) establish communication preferences for Customer; and e) identify key stakeholders from Customer and their role in Service delivery.

8.2.2 **Installation of Service Software**. Once Service Software is installed and activated, the Security Services Team will utilize Service Software to perform Detection, Investigation, and Response Actions. Until Service Software is installed in the Customer's environment, the Security Services Team will only be able to provide technical advice and guidance for Incident triage and response planning. If Deployment is being supported by the Supplier and/or the Services Security Services Team procured by the Supplier by way of Professional Services, it will assist the Customer or Partner with installation of Service Software in accordance with **Schedule 4.2**. The Customer expressly agrees that any unused hours for Deployment will expire after the Rapid Response Subscription Term and payment for Deployment is non-refundable.

8.2.3 **Threat Triage**. The Threat Response Lead will work with the Customer to: a) conduct an assessment of Customer's operating environment; b) understand any threat intelligence and/or other indicators of compromise or indicators of attack; c) perform the necessary data collection, which may include supplemental data (as further described in paragraph 6.1.4; and d) initiate investigative activities and collaborate on a plan for initiating Response Actions.

8.2.4 **Threat Neutralization.** Additional investigation will be conducted, and Response Actions will be performed to: a) remove the attacker's access; b) stop further damage to compromised assets or data; c) recommend preventative actions to address the cause of the Incident; and d) monitor the compromised assets and data to detect reoccurrence.

8.2.5 **Remote Access Tools**. To support Service delivery, the Security Services Team may utilise Sophos owned or selected remote access tools to access or make changes to Managed Endpoints and may utilise administrative access to the Customer's Sophos Central environment to view to modify configurations. Access will be subject to the Customer, approval if the Customer has selected "Authorize" Threat Respond Mode. All access by the Security Services Team to Managed Endpoints and Sophos Central is recorded and logged.

8.3 THE CUSTOMER ACKNOWLEDGES AND AGREES THAT ITS AUTHORIZATION FOR SOPHOS AND THE SUPPLIER TO MAKE ANY CHANGES TO, OR MODIFY CONFIGURATIONS IN, CUSTOMER'S ENVIRONMENT COULD RESULT IN INTERRUPTION OR DEGRADATION OF CUSTOMER'S SYSTEMS AND INFRASTRUCTURE.

8.4 THE CUSTOMER FURTHER ACKNOWLEDGES THAT FAILURE TO GRANT AUTHORISATION FOR SUCH CHANGES COULD RESULT IN NEW MALICIOUS ACTIVITY OR THE WORSENING OF EXISTING MALICIOUS ACTIVITY IF THE CUSTOMER HAS DENIED SOPHOS' OR THE SUPPLIER'S REQUEST FOR AUTHORISATION TO MAKE CHANGES OR MODIFICATIONS.

8.5 The service components referred to at paragraph 5.1.4 to 5.1.5 are not included in Rapid Response Service in relation to the Incident which is present at the point of Order.

SERVICE COMPLETION

8.6 The Rapid Response phase of the Service concludes when the Incident present at the point of Order of Rapid Response is neutralized. Sophos will provide written notification upon completion of the Service to Customer. Upon completion of the Rapid Response phase of the Service, Customer will be provided with the MDR Complete Service for the remainder of the Rapid Response Minimum Term.

THREAT SUMMARY

8.7 After completion of the Rapid Response Service, Sophos will deliver a written threat summary containing the following: a) a summary of investigation activities; b) technical findings; c) analysis of identified threats; d) threat specific remediation/mitigation steps; and e) general recommendations. Customer must within ten (10) days of receipt of the foregoing threat summary, provide written acknowledgement of completion of the Service. The Customer's failure to acknowledge completion of the Rapid Response Service or to provide reasons for refusing to confirm completion within the ten (10) day period will be deemed as Customer's acceptance of completion of the Service.

9. RAPID RESPONSE CUSTOMER RESPONSIBILITIES

9.1 The Customer acknowledges and agrees that it must take the actions listed at paragraph 6 and 9.2 below to facilitate and enable delivery of the Rapid Response Service, and the Supplier and Sophos shall have no liability for any degraded, incomplete, or failed Service delivery which may result from Customer's failure to take required actions.

9.2 During the Rapid Response Phase, the Customer will:

9.2.1 ensure that personnel are always available to enable Sophos to access all supporting data required for analysis from Customer. Such supporting data includes, but is not limited to: a) endpoint, server or network logs, b) architecture diagrams, and c) materials and resources related to Customer's business and technical environment. Supporting data removal from Sophos systems will be initiated upon Customer's written request; and

9.2.2 select the "Authorize" Threat Response Mode in Sophos Central.

10. THREAT ADVISER SERVICE DESCRIPTION

10.1 The Threat Adviser Service monitors alerts from supported MDR Compatible Sophos Products and Third-Party Systems and includes the following:

10.1.1 **Onboarding**. During the onboarding process, the following activities must be performed by the Customer as a precondition to delivery of the Security Service:

10.1.1.1 provide contact information;

10.1.1.2 confirm communication preferences; and

10.1.1.3 configuration of any Third-Party Systems.

10.1.2 **Investigation and Escalation.** Sophos will conduct the following Investigation and Analysis activities for Cases originating from MDR Compatible Sophos Products and Third-Party Systems:

10.1.2.1 Analysis is conducted to enhance identification, aggregation, and prioritisation of Detections resulting in machine generated Cases;

10.1.2.2 Investigations are performed to confirm threats, and Remediation Guidance is provided where applicable. No remediation actions are taken by the Security Services Team or the Supplier;

10.1.2.3 Notification and information about the Case is shared with the Customer based on its pre-selected communication preferences;

10.1.2.4 All monitoring and investigation this paragraph 10.1.2 will be provide on a 24/7/365 basis;

10.1.2.5 The following service level targets are used to provide Customers with guidelines around timing expectations for Case creation and notification resulting from Investigations. These targets only apply to Investigations on Third-Party Systems;

Target time for Case creation	2 minutes from Detection
Target time for initial Response Action	30 minutes from Case creation

11. THREAT ADVISER CUSTOMER RESPONSIBILITIES

11.1 The Customer must take the actions listed at paragraph 10.1 and 11.2 to facilitate and enable delivery of the Threat Adviser Service, and the Supplier and Sophos shall have no liability for any degraded, incomplete, or failed Service delivery which may result from Customer's failure to take required actions.

11.2 The Customer will:

11.2.1 **Onboarding.** The Customer will perform all required activities during the onboarding process and maintain a valid and active Sophos Central account;

11.2.2 **Remediate Incidents.** The Customer must make reasonable efforts to timely remediate any Incident reported by Sophos or by other third-party technologies utilised by the Customer for cybersecurity protection and detection. The Supplier and Sophos will not be liable for any issued caused by the Customer's failure to take remediation steps in a timely manner. Additionally, the Security Services Team has no obligation to notify the Customer or generate new cases from Detections for which Sophos has already provided recommended remediation steps;

11.2.3 **Customer Personnel.** The Customer must identify an appropriate number of suitably skilled personnel who will work with the Supplier and Sophos during the provision of Services. The Customer's personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service;

11.2.4 **Timely Response.** The Customer must promptly acknowledge receipt of Sophos communications in writing (via email or other agreed method) and must timely respond to the Suppliers and Sophos' requests.

11.2.5 **Actions Outside the Scope of Service.** All activities that are not expressly provided for in this Schedule are outside of the scope. The Customer is solely responsible and liable for:

11.2.5.1 neutralizing any Incidents and/or confirmed threats in Third-Party Systems that cannot be resolved by Sophos;

11.2.5.2 taking any actions that are outside the scope of the Service e.g., Sophos suggested on-site response, e-discovery and litigation and collaboration with law enforcement;

11.2.5.3 for any actions undertaken by the Supplier or Sophos that are not provided in this Schedule but which are under the Customer's specific direction; and

11.2.5.4 any security incidents, threats or compromises that occurred or existed prior to the Commencement Date of the Service.

11.2.6 **Non-Sophos Systems.** The Customer acknowledges that Sophos and the Supplier:

11.2.6.1 are not responsible for any changes made to any non-Sophos systems by their vendors or any party that impact either the integration with Service or Sophos' ability to the provide the Service;

11.2.6.2 may, at their discretion, add, remove, and modify supported non-Sophos systems and it is the Customer's responsibility to check the supported list;

11.2.6.3 are not responsible for any Third-Party Systems integrations function and continue to

function properly throughout the duration of the Agreement; and

11.2.6.4 if Third-Party Systems have not been properly configured or do not support transmission of security telemetry to Sophos, Sophos will reasonably work with the Customer to enable security telemetry transmission.

12. GENERAL CUSTOMER RESPONSIBILITIES

12.1 Irrespective of whether the Customer has procured the Products from the Supplier, the obligations and restrictions detailed at paragraphs 5 of **Schedule 3.6 (B) Sophos Endpoint and Security Protection Products** form part of, and are incorporated into, this Schedule as contractual obligations and restrictions deemed applicable to use of the Products with the Managed Security Services.

12.2 The Customer acknowledges and agrees that, they must take the following actions to facilitate and enable delivery of the Service;

12.2.1 the Customer must: a) have a valid, active Sophos Central account, b) deploy and configure the Service Software to Managed Endpoints, and c) maintain compliance with all the requirements identified in Health Checks;

12.2.2 the Customer must make reasonable efforts to timely remediate any compromises reported by Sophos or by other third-party technologies that Customer utilizes for cybersecurity detection and protection;

12.2.3 the Customer must ensure that all Managed Endpoints have accurate time and date settings. Sophos will not be responsible for errors, issues, and residual risk experienced or incurred by Customer for Detections generated by Managed Endpoints with inaccurate time and date settings;

12.2.4 the Customer must identify an appropriate number of suitably skilled personnel who will work with Sophos during the provision of the Service. Customer's personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service; and

12.2.5 the Customer must promptly acknowledge receipt of Sophos communications in writing and must timely respond to Sophos's requests.

13. SERVICE USE AND RESTRICTIONS

RIGHT TO ACCESS AND USE

13.1 The scope of Managed Security Services is limited to the Customer's internal information security environment. The Customer acknowledges and agrees that the Services shall be used for the Customer's own information security purposes only.

13.2 The Customer may permit its Affiliates and End Users to use the Services in accordance with this Schedule, provided that the Customer remains fully responsible and liable for their use and compliance with the terms and conditions of this Schedule.

13.3 Where the Customer is in breach of its obligations under this Schedule, the Supplier and Sophos reserve the right to suspend Service delivery until such time as Customer has remedied such breach.

13.4 Save where the Customer has an Order for **Professional Services**, the Customer is solely responsible for taking any actions suggested by Sophos that are outside of the scope of the Service (e.g., Sophos's suggestions regarding on-site response, litigation and e-Discovery support, and collaboration with law enforcement).

14. CHARGES AND PAYMENT

14.1 This paragraph 14 is supplemental to clause 6 of the **General Conditions** and in the event of express conflict this clause shall take precedence.

14.2 For **Advance Subscriptions**, the Supplier shall invoice the Charges for the full Minimum Term in advance.

14.3 For **Pay Monthly Subscriptions**, the Supplier shall invoice the Customer monthly in arrears in relation to actual usage by the Customer and its End Users in the preceding month based on the applicable Charges as per the Supplier's Tariff at the time of invoice.

14.4 The Charges for each Product detailed in the Order shall be indicative and estimated. The actual fees may vary depending on usage, date of purchase, currency, and inflation.

14.5 The Customer shall pay the Supplier all reasonable and properly incurred expenses, including but not limited to travel and other out of pocket expenses and reasonable time spent by the Engineer(s) in travelling, where the distance travelled is further than 35 miles from the Chess Office closest to the geographical location of the Customer Site.

USE LEVEL

14.6 The Service Entitlement together with the defined Security Service unit(s) or meter(s) specified in the Licensing Guidelines form the applicable Customer use level ("**Use Level**").

14.7 The Customer may access and use the Security Services in accordance with the applicable Use Level and may not exceed the Use Level at any time.

14.8 If Customer wishes to increase its Service Entitlement, it may place an Order with the Supplier. If the Customer exceeds its Service Entitlement, the Customer will pay any invoice for such excess use issued by the Supplier in accordance with clause 6 of the General Conditions.

14.9 Actual usage may vary from month to month and will not be charged on a pro-rata basis. The Supplier reserves the right to charge the Customer a minimum fee of £50 each calendar month, regardless of the actual usage.

14.10 Where the Supplier identifies that the Customer has underpaid the fees, the Customer shall be invoiced for and shall pay the Supplier within seven (7) days of the date of invoice an amount equal to the shortfall between the fees due and those paid.

14.11 If the Customer fails to pay the Supplier by the due date, in addition to Supplier's other rights, the Supplier may require the Customer to purchase Managed Security Services on an Advance Subscription basis.

15. WARRANTIES

15.1 The Supplier warrants only that:

15.1.1 it will provide the Services using commercially reasonable skill and care; and

15.1.2 the Services will materially confirm to the Documentation.

EXCLUSIONS

15.2 The above warranties will not apply if:

15.2.1 the Product or Service has not been used in accordance with this Schedule, Schedule 3.6(B), the End User Terms or the Documentation,

15.2.2 the issue has been caused by failure to apply Updates, Upgrades or any other action or instruction recommended by Sophos and/or the Supplier,

15.2.3 the issue has been caused by the act or omission of, or by any materials supplied by the Customer, its End Users or any third party, or

15.2.4 the issue results from any cause outside of Sophos and/or the Supplier's reasonable control.

REMEDY

15.3 THE SUPPLIER'S ENTIRE LIABILITY AND THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY, FOR BREACH OF THE ABOVE WARRANTIES, SHALL BE (AT THE SUPPLIER'S OPTION AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW) EITHER TO:

15.3.1 TO CORRECT, REPAIR OR REPLACE THE RELEVANT ASPECT OF THE SERVICES OR DOCUMENTATION AS APPLICABLE, WITHIN A REASONABLE TIME, OR

15.3.2 PROVIDE OR AUTHORISE A PRO RATA REFUND OF THE CHARGES PAID FOR THE PERIOD IN WHICH THE SUPPLIER WAS IN BREACH OF THE APPLICABLE WARRANTY.

15.4 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE WARRANTIES IN THIS PARAGRAPH 15 ARE PERSONAL TO THE CUSTOMER AND ARE NOT TRANSFERABLE.

16. INDEMNITY

16.1 The Supplier will:

16.1.1 defend, indemnify, and hold the Customer harmless from any third-party claim, action, suit or proceeding alleging that the Customer's access or use of the Managed Security Services in accordance with the terms and conditions of this Schedule infringes such third party's patent, trademark or copyright;

16.1.2 reimburse the Customer's reasonable legal fees and costs actually incurred and any damages finally awarded against the Customer by a court of a competent jurisdiction or agreed to by the Supplier in a settlement.

16.2 If any such third party claim or proceeding is made or appears likely to be made against the Customer, the Supplier, in its sole discretion, may:

16.2.1 procure the right for the Customer to continue access and use of the applicable Managed Security Services in accordance with the terms and conditions of this Schedule, or;

16.2.2 modify or replace the applicable Managed Security Services to be non-infringing without material decrease in functionality.

16.3 If the Supplier, in its sole discretion, determines that neither the foregoing options is commercially reasonable basis, the Supplier may terminate the Managed Security Services and right to access or use the Services upon notice to the Customer and provide a pro rata refund of fees paid for such Services which:

16.3.1 relates to the period after the date of termination in the case of subscription term Managed Security Services, and;

16.3.2 is depreciated on a straight line five (5) year basis commencing on the date of purchase in the case of perpetual term Managed Security Services.

EXCLUSIONS

16.4 The Supplier will have no indemnity obligation for any claim or proceeding if:

16.4.1 the Customer fails to notify the Supplier in writing within seven (7) days of being notified of any such claim or proceeding;

16.4.2 the Customer does not, at the Supplier's written request, immediately cease to access and use the applicable Managed Security Services and require End Users to do the same;

16.4.3 the Customer, without the Supplier's prior written consent, acknowledges the validity of or takes any action which might impair the ability of the Supplier or Sophos to contest the claim or proceedings;

16.4.4 the infringement arises due to modification of the Managed Security Services by anyone other than the Supplier or Sophos; access or use of the Managed Security Services other than in accordance with the Documentation or in a manner that violates the terms of this Schedule; or combination, operation, or use of the Managed Security Services with any products, services or business processes not provided by the Supplier, if the claim would not have occurred but for such combination, operation or use, or

16.4.5 the claim is raised based on access, use or possession in or from a country that is not a party to the World Intellectual Property Organization (WIPO) treaties on patents, trademarks and copyrights; or

16.4.6 the claim is based on Customer Content, Third Party Products, or Third-Party Services.

CUSTOMER INDEMNITY

16.5 The Customer will indemnify, defend and hold harmless the Supplier, its Affiliates, and their officers, directors, employees, contractors and agents against any claims, liabilities and expenses (including legal fees) that are incurred as a result of or in connection with:

16.5.1 Customer Content;

16.5.2 a breach of **Schedule 3.6(B)** or the Customer's representations and warranties under this Schedule;

16.5.3 the Customer or its End Users access or use of the Managed Security Services in a manner not expressly permitted by this Schedule;

16.5.4 the Customer or its End Users violation of any third party rights;

16.5.5 the Customer or its End Users violation of Applicable Law, or;

16.5.6 any work product created in resilience on the Managed Security Services and use of such work products by the Customer, its End Users or a third party.

INDEMNIFICATION PROCEEDURES

16.6 The indemnified party ("**Indemnitee**") will:

16.6.1 promptly notify the indemnifying party ("**Indemnitor**") in writing of any indemnifiable claim;

16.6.2 give the Indemnitor all reasonable assistance, at Indemnitors expense, and;

16.6.3 give Indemnitor sole control of the defence and settlement of the claim.

16.7 Any settlement of a claim will not include a specific performance obligation other than the obligation to promptly cease using the Managed Security Services, or an admission of liability by the Indemnitee, without the Indemnitee's consent.

16.8 The Indemnitee may join the defence of an indemnifiable claim with legal representation of its choice at its own expense.

16.9 Paragraphs 16.1, 16.2 and 16.3 set out the Customer's sole remedy and the whole liability of the Supplier in the event that the Managed Security Services are alleged to infringe the patents, trademarks, copyrights, or other intellectual property rights of any third party.

17. DISCLAIMER OF WARRANTIES

17.1 EXCEPT FOR THE EXPRESS WARRANTIES FOR THE MANAGED SECURITY SERVICES CONTAINED IN PARAGRAPH 15.1 ABOVE, THE SUPPLIER, ITS THIRD PARTY LICENSORS, AND ITS SUPPLIERS MAKE NO WARRANTIES, CONDITIONS, UNDERTAKINGS OR REPRESENTATIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE IN RELATION TO THE MANAGED SECURITY SERVICES OR ANY THIRD PARTY SOFTWARE INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, UNINTERRUPTED USE, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR ARISING FROM COURSE OF DEALING, USAGE OR TRADE.

17.2 WITHOUT LIMITATION TO THE FOREGOING, THE SUPPLIER, ITS THIRD-PARTY LICENSORS, AND ITS SUPPLIERS DO NOT WARRANT THAT THE MANAGED SECURITY SERVICES WILL:

17.2.1 MEET THE CUSTOMER'S REQUIREMENTS;

17.2.2 BE ERROR FREE, FAILSAFE OR UNINTERRUPTED;

17.2.3 DETECT, CORRECTLY IDENTIFY AND/OR REMEDIATE ALL THREATS, APPLICATIONS (WHETHER MALICIOUS OR OTHERWISE) OR OTHER COMPONENTS.

17.3 FURTHER, THE SUPPLIER, ITS THIRD-PARTY LICENSORS AND ITS SUPPLIERS DO NOT WARRANT OR REPRESENT THAT THE CUSTOMER OR ANY END USER IS ENTITLED TO BLOCK ANY THIRD-PARTY APPLICATIONS OR THAT THE CUSTOMER IS ENTITLED TO ENCRYPT OR DECRYPT ANY THIRD-PARTY INFORMATION OR THAT DEFECTS IN THE MANAGED SECURITY SERVICES WILL BE CORRECTED.

17.4 THE SUPPLIER DISCLAIMS ANY RESPONSIBILITY FOR ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE MANAGED SECURITY SERVICES THAT ARISE FROM CUSTOMER CONTENT, THIRD PARTY SOFTWARE, THIRD PARTY SERVICES, OR ANY OTHER SERVICES PROVIDED BY THIRD PARTIES, OR FOR ANY INTERCEPTION OR INTERRUPTION OF ANY COMMUNICATIONS THROUGH THE INTERNET, NETWORKS, OR SYSTEMS OUTSIDE OF THE SUPPLIER'S CONTROL.

17.5 THE CUSTOMER FURTHER ACKNOWLEDGES AND AGREES THAT IT SHALL BE SOLELY RESPONSIBLE FOR PROPER BACK-UP OF ALL DATA AND THAT THE CUSTOMER SHALL TAKE APPROPRIATE MEASURES TO PROTECT SUCH DATA. THE SUPPLIER, ITS THIRD-PARTY LICENSORS AND ITS SUPPLIERS ASSUME NO LIABILITY OR RESPONSIBILITY WHATSOEVER IF DATA IS LOST OR CORRUPTED.

18. LIMITATION OF LIABILITY

18.1 THIS PARAGRAPH 18 IS SUPPLEMENTAL TO 9 OF THE **GENERAL CONDITIONS** AND IN THE EVENT OF AN EXPRESS CONFLICT ONLY SHALL THIS PARAGRAPH 18 TAKE PRECEDENCE.

18.2 SOPHOS AND THE SUPPLIER SHALL HAVE NO LIABILITY FOR ANY DEGRADED, INCOMPLETE, OR FAILED SERVICE DELIVERY WHICH MAY RESULT FROM CUSTOMER'S FAILURE TO COMPLY WITH ITS OBLIGATIONS AS DETAILED IN THIS SCHEDULE, **SCHEDULE 3.6(B),** OR THE **END USER TERM** AS APPLICABLE.

18.3 THE CUSTOMER AND ITS END USERS ACCEPT THAT USE OF THE MANAGED SECURITY SERVICE IS AT ITS OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE SUPPLIER BE LIABLE TO FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES OR LOSS OF ANY KIND INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, LOSS OF CONTRACTS, BUSINESS INTERRUPTIONS, LOSS OF OR CORRUPTION OF DATA HOWEVER CAUSED, EVEN IF THE DAMAGES WERE FORESEEABLE OR THE SUPPLIER HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

18.4 IN NO EVENT WILL THE AGGREGATE LIABILITY OF THE SUPPLIER FOR DIRECT DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE MANAGED SECURITY SERVICE, EXCEED A SUM EQUAL TO THE CHARGES PAID OR PAYABLE BY THE CUSTOMER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

18.5 THE LIMITATIONS AND EXCLUSIONS OF LIABILITY UNDER THIS PARAGRAPH 18 APPLY:

18.5.1 WHETHER SUCH CLAIM ARISES UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY, STATUTE OR OTHERWISE, AND;

18.5.2 NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY

NOTHING IN THIS SCHEDULE LIMITS OR EXCLUDES ANY LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

19. THIRD PARTY SOFTWARE AND SERVICES

19.1 The Products used to provide the Managed Security Services may operate or interface with software or other technology that is licensed to the Supplier or Sophos from third parties ("**Third Party Licensors**"), which is not proprietary to Sophos, but which Sophos and the Supplier has the necessary rights to license ("**Third Party Software**").

19.2 The Customer agrees that:

19.2.1 the Customer and its End Users will use such Third-Party Software in accordance with this Schedule;

19.2.2 no Third-Party Licensor makes any warranties, conditions, undertakings or representations of any kind, either express or implied, to the Customer or its End Users concerning such Third-Party Software or the Managed Security Services themselves;

19.2.3 no Third-Party Licensor will have any obligation or liability to the Customer or its End Users as a result of this Schedule or use of such Third Party Software;

19.2.4 the Third-Party Licensor is a beneficiary of this Schedule and accordingly may enforce the terms and conditions herein to the extent necessary to protect its rights in relation to the Third-Party Software, and;

19.2.5 such Third-Party Software may be licensed under license terms which grant additional rights or

contain additional restrictions in relation to such materials, beyond those set forth in this Schedule,

and such additional license rights and restrictions are described or linked to in the applicable Documentation, the relevant Sophos webpage, or within the Managed Security Services itself.

19.3 For the avoidance of any doubt, such additional rights and/or restrictions apply to the Third-Party Software on a standalone basis. Nothing is such third-party licenses shall affect the Customer or its End Users use of the Managed Security Services in accordance with the terms and conditions of this Agreement.

19.4 Where the Product includes Java Software ("**Java**") from Oracle Corporation ("**Oracle**"), use of the commercial features for any commercial or production purpose requires a separate license from Oracle. Commercial Features means those features that are identified as such in the Licensing Information User manual – Oracle Java SE and Oracle Java Embedded Products Document which can be found at https://www.oracle.com/java/technologies/javase-documentation.html, under the "*Description of Products Editions and Permitted Features*" section.

19.5 The Customer acknowledges that Google Maps / Google Earth Additional Terms of Service https://maps.google.com/help/terms_maps/ (including the Google Privacy Policy https://policies.google.com/privacy) apply to MSP's and Beneficiaries' use of Sophos Central Wireless.

19.6 The Services may enable or require the Customer to associate its Service account with, link to, or otherwise access, third parties' websites, platforms, content, products, services or information ("**Third-Party Services**"). Third-Party Services are not part of the Services and neither Sophos or the Supplier control or are responsible for the Third-Party Services. The Customer is solely responsible for:

19.6.1 obtaining and complying with any terms of access and use of the Third-Party Services including paying any Charges; and

19.6.2 configuring the Third-Party Services appropriately.

19.7 The Supplier disclaims all liability arising from or related to the Customer's access or use of the Third-Party Services including any impact on Service capabilities as a result of any use of, or reliance upon, the Third-Party Services.

20. TERM AND TERMINATION

20.1 This paragraph 20 is supplemental to clause 8 of the **General Conditions** and in the event of express conflict shall supersede it.

20.2 Where the Agreement relates to a **Pay-Monthly Subscription** and such Agreement is terminated by the Customer within its Minimum Term, the Supplier shall be entitled to invoice the Customer for Termination Charges in accordance with clause 8.7 of the **General Conditions**.

20.3 The Supplier may terminate this Schedule immediately upon written notice if:

20.3.1 it does not receive the fees (in whole or in part) from the Customer in accordance with the agreed payment terms, or

20.3.2 the Customer fails to comply with any of the terms and conditions of this Schedule, or

20.3.3 the Supplier takes or suffers any action on account of debt or become insolvent.

EFFECTS OF TERMINATION

20.4 Termination of this Schedule shall not relieve the Customer of its obligations to pay all Charges that have accrued or are otherwise owed by the Customer to the Supplier. All Charges paid whether by way of an Advanced Subscription or otherwise are non-refundable to the maximum extent allowed by Applicable Law.

20.5 The following paragraphs of this Schedule, together with any terms necessary for the interpretation of the Agreement, will survive termination or expiry of the Agreement 16, 17, 18, 19, 20, 21, 22.

21. CONFIDENTIALITY AND DATA PROTECTION

21.1 This paragraph 21 supplemental to clauses 10 and 12 of the **General Conditions**, in the event of express conflict only it shall supersede the **General Conditions**.

21.2 The Customer agrees that the Supplier or Sophos may send promotional emails to the Customer to provide information about other goods and services which may be of interest. The Customer may notify the Supplier that you wish to withdraw permission for such promotional emails at any time by sending an email to marketing@chessICT.co.uk.

21.3 The Customer acknowledges and agrees that the Supplier and Sophos may directly and remotely communicate with the Products to provide Managed Security Services, and to collect the following types of information:

21.3.1 Products, Product versions, Product features and operating systems being used;

21.3.2 processing times taken by the Product;

21.3.3 customer identification code and company name;

21.3.4 IP address and/or ID of the machine which returns the above listed information, and;

certain Products may require the collection of additional information as detailed in the Sophos Group Privacy Notice and Data Processing Addendum at https://www.sophos.com/en-us/legal/sophos-group-privacy-notice.

USAGE DATA AND THREAT INTELLIGENCE DATA

21.4 The Supplier and Sophos may collect, access, use, process, transmit, or store Usage Data and information collected under paragraph 21.3 may be used for the purposes of:

21.4.1 providing the Managed Security Services, performing this Schedule 4.6(C) and the Agreement;

21.4.2 verifying Customer compliance with this Agreement and Schedule 3.6(B) where applicable;

21.4.3 evaluating and improving the performance of the Products and Managed Security Services;

21.4.4 preparing statistical analysis (such as malware infection rates and the usage of Products) that is aggregated, anonymised, de-identified or otherwise rendered not reasonably associated or linked to identifiable individual and using such analysis for the purposes of raising awareness of security risk and security threat research; and

21.4.5 issuing alerts and notices about incidents and product lifecycle changes which affect the Products being used.

21.5 The Supplier and Sophos requires, and the Customer agrees to provide, complete and accurate identification information and (where applicable) payment information for the purposes of:

21.5.1 providing technical support;

21.5.2 billing;

21.5.3 verifying Credentials;

21.5.4 issuing license expiry and renewal notices, and

21.5.5 providing account management.

21.6 In the case of personal data processed on behalf of the Customer, the Supplier acts as a Data Processor. In the case of personal data used for the Supplier or Sophos business purposes under paragraphs 21.3 and 21.4, the Supplier or Sophos is the Data Controller, as applicable.

21.7 The terms "Processor" and "Controller" shall have the meanings defined in the General Data Protection Regulation ("**GDPR**"). The Supplier will process any personal data in accordance with the provisions of GDPR and its Privacy Notice. As a global organization, the group companies, subcontractors, suppliers and third-party licensors of Sophos may be located anywhere in the world. Sophos will process any personal data in accordance with the provisions of GDPR and the Sophos Group Privacy Notice and Data Processing Addendum.

21.8 The Customer hereby acknowledges and provides its consent for the Products to intercept, access, monitor, log, store, transfer, export, block access to, and/or delete the Customer's communications or the communications of its Users.

21.9 The Customer expressly confirms its consent to the use of data and information as set forth herein and in the group Privacy Notice and Data Processing Addendum, and further warrant that the Customer has obtained all necessary consents and provided all necessary notifications to share such data and information with the Supplier and Sophos for the purposes described above.

21.10 Each party shall take appropriate technical and organizational measures against unauthorized or unlawful processing of personal data or its accidental loss, destruction or damage.

21.11 The Customer agrees to indemnify and hold the Supplier harmless from and against any liability that arises in relation to the Customer's failure to comply with this paragraph 21 and/or the **General Conditions**.

22. EXPORT CONTROL

22.1 The Customer:

22.1.1 agrees that in connection with its use of the Products it will comply, and its Personnel, will comply with all Sanction and Export Control Laws;

22.1.2 represents and warrants it will not export, re-export, transfer or otherwise make available the Products directly or indirectly to (i) any country or region which is subject to sanctions or trade embargos administered and enforced by the European Union, United Kingdom and the United States; (ii) any individual or entity which is on a restricted persons list maintained by the European Union, United Kingdom and the United States; or (iii) to target or subject of any Sanctions or Export Control Laws;

22.1.3 understands and agrees that the Supplier and Sophos shall have no obligation to provide the Products or any services where the Supplier believes it could violate Sanctions or Export Control Laws; and

22.1.4 agrees that any breach of this paragraph 22 shall be a material breach incapable of remedy and cause for immediate termination and agrees to indemnify the Supplier and hold the Supplier harmless from and against claims, loss, liability or damage suffered or incurred by the Supplier resulting from or related to the violation of this paragraph 22 by the Customer, its End Users or its Personnel.

23. GENERAL

23.1 The Customer acknowledges and agrees that Sophos may vary, Update or discontinue Products, Product versions, Product features, Support or Managed Support Services, and support for Third Party Software (including without limitation operating systems and platforms) from time to time for reasons including but not limited to changes in demand, security and technology.

ANNEX 1 – DEFINITIONS

"Advanced Subscription" means a License Subscription for either a 12- or 36-month period as stated on the Order and where the License Charges are payable in full and in advance for the duration of the Subscription;

"**Case**"

(i) in relation to MDR and MDR Complete, is a Detection or set of Detections that has high severity level and warrants human review. Cases can be (i) generated automatically by policies or analytics applied to telemetry from Managed Endpoints and Third-Party Systems, (ii) identified through Threat Hunting activities; or (iii) manually created at the discretion of the Security Services Team or at the request of the Customer;

(ii) in relation to Threat Response, is a Detection or set of Detections that has high severity level and warrants human review. Cases can be (i) generated automatically by policies or analytics applied to telemetry from Managed Endpoints and Third-Party Systems; or (ii) manually created at the discretion of the Security Services Team or at the request of the Customer;

"**Deployment**" is guidance, advice, and remote assistance service offered by Sophos with configuration and deployment of Service Software.

"**Detection**"

(i) in relation to MDR and MDR Complete, is a condition where data generated by a Managed Endpoint or Third-Party Systems is identified as an indicator of malicious or suspicious activity;

(ii) in relation to Rapid Response, is a condition where data generated by a Managed Endpoint is identified as an indicator of malicious or suspicious activity;

(iii) in relation to Threat Response, is a condition where data generated by MDR Compatible Sophos Products or Third-Party Systems is identified as an indicator of malicious or suspicious activity.

"**Documentation**" means any online help content, user manuals, or similar materials pertaining to the implementation, operation, access and use of the Services or Products that are made available by the Supplier and/or the Sophs, as may be revised from time to time;

"End User Terms" means the Sophos End User Terms of Use, service agreement, or other terms of access and use applicable to each Products that accompanies the Products, is published at https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use.

"**Health**"

(i) in relation to MDR and MR Complete, is the state of configurations and settings for the Managed Endpoint running Sophos Intercept X with XDR that affect the efficacy of the security of the Managed Endpoint;

(ii) in relation to Rapid Response, is the state of configurations and settings for the Managed Endpoint that affect the efficacy of the security of a Managed Endpoint;

"**Health Check**" is the act of reviewing Health to identify configurations and settings that may negatively impact the efficacy of the security of the Managed Endpoint.

"**Incident**" is a confirmed compromise or unauthorised access of a system or systems that poses an imminent threat to Customer assets which includes interactive attackers, data encryption or destruction and exfiltration.

"**Incident Response Lead**" is a member of the Sophos Security Services Team who is identified as the primary individual for assisting a Customer during Incident Response"

"**Incident Response**" is the technical process performed remotely by the Security Services Team to Investigate, mitigate and neutralize an Incident.

"**Investigation**"

(i) in relation to MDR and MDR Complete and Rapid Response, means a formal process and methods used by the Security Services Team to confirm whether activity in a Case is malicious and requires Threat Response;

(ii) in relation to Threat Response, means a formal process and methods used by the Security Services Team to confirm whether activity in a Case is malicious;

"**Products**" means Sophos Endpoint and Security Protection Products as further described in Schedule 3.6(B).

"**Managed Endpoint**"

(i) in relation to MDR and MDR Complete, is any physical or virtual endpoint device or server system where Sophos Intercept X Advanced with XDR or Sophos XDR Sensor is installed, up-to-date, and operational in support of Service delivery;

(ii) in relation to Rapid Response, any physical or virtual device or a server system where the Service Software is installed, up-to-date, and operational in support of Service delivery;

"**MDR Compatible Sophos Products**" refers to any Sophos product that send telemetry and alerts to Sophos Central that can be used to support Service delivery.

"**Pay-Monthly Subscription**" means a License Subscription whereby the Customer is provided with the Subscription on a monthly basis and is charged on a monthly basis for the Minimum Term;

"**Remediation Guidance**" means guidance provide by Sophos or the Supplier regarding actions that may be taken by the Customer on MDR Compatible Sophos Products or Third-Party Systems in order to help mitigate or resolve an Incident;

"**Response Action**"

(i) in relation to MDR and MDR Complete, is an interaction with Managed Endpoints to perform Investigation and Threat Response, including but not limited to remote query, host isolation, terminating a process, blocking an IP address and deleting malicious artefacts. Escalation using pre-selection preferences shall also be deemed Response Action;

(ii) in relation to Rapid Response, is an interaction with Managed Endpoints to perform Investigation and Threat Response, including but not limited to remote query, host isolation, terminating a process, blocking an IP address and deleting malicious artefacts;

"**Security Services Team**"

(i) in relation to MDR, MDR Complete and Rapid Response, is the Sophos team conducting security Investigations, Threat Hunting, Response Actions and Incident Response where applicable;

(ii) in relation to Threat Response, is the Sophos team conducting security Investigations and recommending Remediation Guidance;

"**Termination Charges**" means compensatory Charges payable by the Customer to the Supplier on termination of this Agreement in whole or in part pursuant to clause 8.7 of the **General Conditions**, being an amount equal an average of the monthly Charges invoiced by the

Supplier in the 6 months prior to the date of termination, multiplied by the number of remaining months of the **Minimum Term**.

"**Third-Party Remediation Guidance**" means guidance provided by Sophos regarding actions that may need to be taken by the Customer on Third-Party Systems from Customer's security tools to the Service using Sophos integrations and integration mechanisms.

"**Third-Party System**" means supported non-Sophos systems (e.g. endpoints, servers, firewalls etc.) which are configured to send security telemetry from Customer's security tools to the Service using Sophos integrations and integration mechanisms.

"**Threat Hunting**"

(i) in relation to MDR and MDR Complete, is the process of proactively and iteratively searching through data originating from Service Software to identify signals and indicators of malicious activity that may have passed existing prevention and detection controls;

(ii) in relation to Rapid Response, is the process of proactively and iteratively searching through data originating from Service Software using a combination of manual and semi-automated activity to identify signals and indicators of malicious activity that may have passed existing prevention and detection controls;

"**Threat Response**" includes the methods, processes, communications, and Response Actions utilized by the Security Services Team and the Customer, as applicable, to contain or disrupt malicious activity.

"**Threat Response Mode**" is the type of action to be taken by the Security Services Team i.e. Collaborate or Authorize as determined by the Customer during onboarding.