SCHEDULE 4.6 (C) – SOPHOS MANAGED SECURITY SERVICES

1. APPLICATION

1.1 This Schedule, which contains a description of the Managed Security Services which form part of the Agreement entered into 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 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 The provision of Managed Security Services is subject to the Customer purchasing the relevant Licensed Products as set forth in **Schedule 3.6 (B) Sophos Endpoint and Security Protection Products** and the terms and conditions therein shall be deemed to be part of and incorporated into this Schedule.

1.4 To the extent there is a conflict between **Schedule 3.6 (B) Sophos Endpoint and Security Protection Products** and this Schedule, the terms and conditions of this Schedule will take precedence.

2. SERVICE DESCRIPTION

2.1 The Supplier shall provide the Customer with the managed security services, comprising of one or more of the following as set forth in the applicable Order;

2.1.1 Sophos Managed Threat Response ("MTR");

2.1.2 Sophos Rapid Response; or

2.1.3 other associated security services as described in the applicable Service Description

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

2.2 Notwithstanding anything to the anything to the contrary in this Schedule, the Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to https://www.sophos.com/en-us/legal.aspx

3. SERVICE USE AND RESTRICTIONS

RIGHT TO ACCESS AND USE

3.1 Subject to the Customer's compliance with the terms of this Schedule, the Supplier grants the Customer a non-exclusive, non-transferable, worldwide right to access and use the Security Services during the applicable Subscription Term solely for the Customer's internal information security purposes.

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

3.3 The Customer's obligations set forth in paragraphs 4.6 to 4.8 inclusive of **Schedule 3.6 (B) Sophos Endpoint and Security Protection Products** shall form part of and are incorporated into this Schedule under this paragraph 3.3 and the defined term "Products" shall be replaced with "Managed Security Services".

3.4 In addition to paragraph 3.3 above, the Customer acknowledges and agrees that, they must take the following actions to facilitate and enable delivery of the Service, and Sophos shall have no liability for any degraded, incomplete, or failed Service delivery which may result from Customer's failure to do so. Sophos reserves the right to suspend Service delivery until such time as Customer performs the required actions;

3.4.1 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;

3.4.2 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;

3.4.3 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

3.4.4 during the course of providing the Rapid Response Service, the Security Services Team may request additional supporting data, and Customer will ensure that Sophos has access to such supporting data at all times. Such supporting data may include, but is not limited to: ai) 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

3.4.5 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.

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

3.4.7 the Customer must select the "Authorize" Threat Response Mode in Sophos Central for the Rapid Response Service.

3.5 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).

USE LEVEL

3.6 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**").

3.7 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.

3.8 If Customer wishes to increase its Service Entitlement, it must first purchase the corresponding additional Service Entitlement. If the Customer exceeds its Service Entitlement, the Customer will pay any invoice for such excess use issued by the Supplier in accordance with paragraph [6.1].

RESTRICTIONS

3.9 The restrictions set forth in paragraph 4.12 of **Schedule 3.6 (B) Sophos Endpoint and Security Protection Products** shall form part of and incorporated into this Schedule under this paragraph 3.6 and the defined term "Products" shall be replaced with "Managed Security Services".

4. SERVICE DESCRIPTION

MANAGED THREAT RESPONSE ("MTR")

4.1 The MTR Service is provided on Managed Endpoints and includes the following activities:

4.1.1 **Onboarding**. During the onboarding process, the following activities must occur as a precondition to delivery of the Security Service:

(a) the Customer will (i) provide contact information, (ii) determine Customer communication preferences, and (iii) determine the Threat Response Mode;

(b) the Customer will install the required Service Software on all Managed Endpoints to be covered by the Service;

(c) on receipt of the telemetry from a Managed Endpoint, a Health Check will be initiated by the Supplier to determine if the policies configured are suitable for the environment and expected capabilities;

4.1.2 **Investigations and Response**. The following investigation and analysis activities for Detections originating from Managed Endpoints will be conducted by the Supplier:

(a) analysis is conducted to enhance identification, aggregation, and prioritization of Detections, resulting in machine-generated Cases.

(b) cases are reviewed to determine what investigation and Response Actions are appropriate for neutralizing Active Threats.

(c) a formal investigation framework is utilized to supplement Cases with attack intelligence, drive continuous enrichment of Case details, and provide situational awareness throughout the investigation lifecycle.

(d) escalation: information about the Case is shared with the Customer based on Customer's pre-selected communication preferences.

(e) all monitoring, investigation, and Response Actions described in this paragraph 4.1.2 will be provided on a 24/7/365 basis.

(f) the following service level targets are utilized to provide Customers with 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

4.1.3 **Threat Hunting**. Threat Hunting will be conducted on Managed Endpoints to search for undiscovered or new threats, indicators of attack or compromise, or other attacker activities. When a Threat Hunt reveals signals or indicators of malicious activity, a Case is created, investigation is conducted, and upon verification of an Active Threat, Response Actions are initiated.

4.1.4 **Reporting**; Health Monitoring; Notification. Periodically, the Customer will be provided with (a) reports relating to Detections, investigations 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.

4.2 To support Service delivery, the Security Services Team may use 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. Access will be subject to Customer approval, either on a per-escalation basis or based on blanket pre-approval if the Customer has selected the "Authorize" Threat Response Mode. All access by the Security Services Team to Managed Endpoints and Sophos Central is recorded and logged

4.3 Customer acknowledges and agrees that customer's 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.

TIERS OF MTR SERVICE OFFERING

4.4 The Service is offered under two tiers: Standard and Advanced. The Standard tier of the Service includes the scope and benefits described in paragraphs 4.1 to 4.3 above.

4.5 The Advanced tier of the Service includes the Standard tier plus the following:

4.5.1 enhanced Threat Hunting utilizing proprietary methods to anticipate and identify indicators of attack and compromise based on factors specific to Customer's environment;

4.5.2 assignment of a Dedicated Response Lead during Threat Response (Dedicated Response Lead is a named lead per shift on the Security Services Team who is the single point of contact during Threat Response);

4.5.3 direct call-in access to the Security Services Team;

4.5.4 proactive recommendations to prevent or reduce Active Threats;

4.5.5 scheduled discussion with Customer to review MTR capabilities and Cases upon Customer's request; and

4.5.6 analysis of Detections originating from other Sophos Central-managed products via connectors.

RAPID RESPONSE

4.6 Rapid Response is a separate Service offering that is built on the MTR Advanced Service and provides Customers with Threat Response during an Active Threat. All aspects of the Service will be provided remotely. Throughout the Rapid Response Service delivery phase, Rapid Response includes the scope and benefits of MTR Advanced Service (in accordance with Section II above) in addition to the following activities:

4.6.1 **Kick Off.** A kick-off call will be conducted to: a) exchange information about the Active Threat and Customer's existing infrastructure; b) identify the scope and impact of the Active Threat; 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.

4.6.2 **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 Active Threat triage and response planning. If Customer purchases Deployment (separately sold), Security Services Team will assist the Customer or Partner with installation of Service Software. Customer expressly agrees that any unused hours for Deployment will expire after the Rapid Response Subscription Term and payment for Deployment is non-refundable.

4.6.3 **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 Section IV. 4); and d) initiate investigative activities and collaborate on a plan for initiating Response Actions.

4.6.4 **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 Active Threat; and d) monitor the compromised assets and data to detect reoccurrence.

SERVICE COMPLETION

4.7 The Rapid Response phase of the Service concludes when the Active Threat present at the point of purchase 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 Advanced tier of the MTR Service for the remainder of the Rapid Response Subscription Term.

THREAT SUMMARY

4.8 Within (10) days of 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 Sophos's completion of the Service. 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

5. PRICING AND PAYMENT

5.1 The fees 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.

5.2 The Supplier shall raise invoices as follows;

5.2.1 for advance subscription, the Supplier shall invoice the fees for the entire Subscription Term in advance, and;

5.2.2 for monthly subscriptions, monthly in arrears in relation to actual usage by the Customer and its End Users in the preceding month based on the applicable fees at the time of invoice.

5.3 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.

5.4 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.

5.5 In the event that 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.

5.6 Payment of the fees shall be due within seven (7) days of the date of invoice, unless specified otherwise on the applicable Order.

5.7 All payments, fees and other charges payable to the Supplier under this Schedule are exclusive of all taxes, levies and assessments.

6. LICENSED PRODUCT WARRANTIES

6.1 For a warranty period of ninety (90) days from the execution of the relevant Order for the Products ("**Warranty Period**"), the Supplier warrants only that:

6.1.1 if properly used and installed, the Products will perform substantially in accordance with the Documentation on the designated operating system(s), and

6.1.2 the Documentation will adequately describe the operation of the Products in all material respects.

6.2 The Supplier warrants to the Customer only that:

6.2.1 it will provide Standard Support and Maintenance using commercially reasonable skill and care, and;

6.2.2 the Standard Support and Maintenance will materially conform to the Documentation.

EXCLUSIONS

6.3 The above warranties will not apply if:

6.3.1 the Licensed Product or service has not been used in accordance with the terms and conditions of this Schedule and the Documentation,

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

6.3.3 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

6.3.4 the issue results from any cause outside of Sophos and/or the Supplier's reasonable control, or;

6.3.5 the Customer fails to notify the Supplier of a breach of the Licenced Products warranty within the Warranty Period or fails to promptly notify the Supplier of a breach of paragraph 7.2 above.

REMEDY

6.4 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:

6.4.1 to correct, repair or replace the relevant Licensed Products, Documentation, or service as applicable, within a reasonable time, or

6.4.2 provide or authorise a pro rata refund of the Fees paid for the period in which the Supplier was in breach of the applicable warranty.

6.5 To the maximum extent permitted by applicable law, the warranties in this paragraph 5 are personal to the Customer and are not transferable.

7. INDEMNITY

7.1 The Supplier will:

7.1.1 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;

7.1.2 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.

7.2 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:

7.2.1 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;

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

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

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

7.3.2 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

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

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

7.4.2 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;

7.4.3 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;

7.4.4 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

7.4.5 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

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

CUSTOMER INDEMNITY

7.5 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:

7.5.1 Customer Content;

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

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

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

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

7.5.6 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

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

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

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

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

7.7 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.

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

7.9 Paragraphs 7.1, 7.2 and 7.3 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.

8. DISCLAIMER OF WARRANTIES

8.1 Except for the express warranties for the Managed Security Services contained in paragraph X 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.

8.2 Without limitation to the foregoing, the Supplier, its Third Party Licensors and its suppliers do not warrant that the Managed Security Services will:

8.2.1 meet the Customer's requirements;

8.2.2 be error free, failsafe or uninterrupted;

8.2.3 detect, correctly identify and/or remediate all threats, applications (whether malicious or otherwise) or other components.

8.3 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.

8.4 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.

8.5 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.

9. LIMITATION OF LIABILITY

9.1 The Customer and its End Users accept that use of the Managed Security Services is at its own risk. To the maximum extent permitted by Applicable Law, in no event shall the Supplier, their affiliates or any Third Party Licensors and suppliers 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, Sophos or their affiliates had been advised of the possibility of such damages.

9.2 In no event will the aggregate liability of the Supplier, Sophos or their affiliates for direct damages arising out of or in connection with this Schedule or the Managed Security Services, exceed a sum equal to the fees paid or payable by the Customer in the twelve (12) month period immediately preceding the event giving rise to the claim.

9.3 The limitations and exclusions of liability under this paragraph 9 apply:

9.3.1 whether such claim arises under contract, tort (including negligence), equity, statute or otherwise, and;

9.3.2 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.

10. THIRD PARTY SOFTWARE AND SERVICES

10.1 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**").

10.2 The Customer agrees that:

10.2.1 The Customer and its End Users will use such Third Party Software in accordance with this Schedule;

10.2.2 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;

10.2.3 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;

10.2.4 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;

10.2.5 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.

10.3 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 Schedule.

11. TERM AND TERMINATION

11.1 This Schedule shall commence upon execution of the Order and continue unless and until terminated in accordance with the provisions set out herein or as set out in the General Conditions.

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

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

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

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

EFFECTS OF TERMINATION

11.3 Termination of this Schedule shall not relieve the Customer of its obligations to pay all License Fees that have accrued or are otherwise owed by the Customer to the Supplier. All License

Fees paid are non-refundable to the maximum extent allowed by Applicable Law.

11.4 Except as otherwise set forth in this Schedule, within one (1) month after the date of termination of this Schedule, the Customer shall provide written certification to the Supplier confirming:

11.4.1 the destruction by the Customer of all partial and complete copies of the Licensed Products, and;

11.4.2 the Customer's termination of all End Users ability to access and use the services.

11.5 All rights of the Customer and its End Users to access and use the Licensed Products will automatically cease upon termination of this Schedule.

11.6 The Customer's obligations under this Schedule in respect of the intellectual property and confidential information of shall survive any expiry or termination of this Schedule.

12. CONFIDENTIALITY AND DATA PROTECTION

12.1 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.

12.2 The Customer acknowledges and agrees that the Supplier and Sophos may directly and remotely communicate with the Products in order to provide Standard Support and Maintenance, and to collect the following types of information:

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

12.2.2 processing times taken by the Product;

12.2.3 customer identification code and company name;

12.2.4 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 privacy policy at: http://www.sophos.com/en-us/legal/sophos-group-privacy-policy.aspx (the "**Sophos Privacy Policy**").

USAGE DATA AND THREAT INTELLIGENCE DATA

12.3 The Supplier may collect, access, use, process, transmit, or store Usage Data and information collected under paragraph 11.2 may be used for the purposes of:

12.3.1 providing the Products and performing this Schedule 3.6(B);

12.3.2 verifying your compliance with this Schedule 3.6(B);

12.3.3 evaluating and improving the performance of the Products;

12.3.4 preparing statistical analysis (such as malware infection rates and the usage of Products);

12.3.5 planning development roadmaps and product lifecycle strategies, and;

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

12.4 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:

12.4.1 providing technical support;

12.4.2 billing;

12.4.3 verifying Credentials;

12.4.4 issuing license expiry and renewal notices, and

12.4.5 providing account management.

12.5 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 13.3 and 13.4, the Supplier or Sophos is the Data Controller, as applicable.

12.6 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 Privacy Policy.

12.7 The Customer hereby acknowledges and provides its consent for the Licensed 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.

12.8 The Customer expressly confirms its consent to the use of data and information as set forth herein and in the Privacy Notice and Sophos Privacy Policy, 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.

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

12.10 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 13.

13. GENERAL

13.1 The Customer acknowledges and agrees that Sophos may vary, Update or discontinue Products, Product versions, Product features, Standard Support and Maintenance, 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.

13.2 The Supplier recommends that the Customer uses the latest Products, Product versions and/or Third Party Software, as applicable.

ANNEX 1 – DEFINITIONS

"**Active Threat**" is an infection, compromise, or un-authorized access of asset(s) that is attempting to circumvent controls in an effort to compromise a Managed Endpoint.

"**Case**" is a Detection or set of Detections that (i) is generated by a Managed Endpoint for human review, (ii) has been identified through Threat Hunting activities, or (iii) has been manually created at the discretion of the Security Services Team or at the request of the Customer.

"**Cloud Service**" means Sophos Cloud Optix services

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

"**Detection**" is a condition where data generated by a Managed Endpoint has been identified as an indicator of malicious or suspicious activity.

"**Health**" is the state of configurations and settings for the Managed Endpoint that affect the efficacy of the Managed Endpoint.

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

"**Managed Endpoint**" is a desktop or server system where the Service Software is installed, up-to-date, and operational in support of Service delivery.

"**Security Services Team**" is the Sophos team conducting Threat Hunting, investigation, and Response Actions.

"**Response Action**" is an interaction with Managed Endpoints to investigate and neutralize Active Threats, including but not limited to remote query, host isolation, killing a process, blocking an IP address, and deleting malicious code.

"**Threat Hunting**" is the process of proactively and iteratively searching through data originating from Service Software to identify signals and indicators of malicious activity.

"**Threat Response**" includes the methods, processes, communications, and Response Actions utilized by the Security Services Team and the Customer, as applicable, to neutralize Active Threats.

"**Threat Response Lead**" is a member of the Sophos Security Services Team who is identified as the primary individual responsible for assisting a Customer during an Active Threat.

"**Threat Response Mode**" is the approach to notification, collaboration, and Threat Response adopted by the Security Services Team during delivery of the Service per Customer direction.