SOPHOS

SOPHOS END USER TERMS OF USE

This Sophos End User Terms of Use ("Agreement") is effective on the date on which the end customer agrees to purchase the Sophos Products through the Carahsoft GSA Schedule (the "Effective Date"). This Agreement shall be binding as between Sophos Limited, registered in England and Wales number 2096520 with registered offices at The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, United Kingdom ("Sophos"), and the end customer identified in the Ordering Activity submitted to partner/reseller under Carahsoft GSA Schedule, as identified in the Order (the "Customer").

NOW IT IS AGREED as follows:

NON-MATERIAL CHANGES TO THIS AGREEMENT MAY BE MADE BY SOPHOS AND ANY MODIFICATION OR UPDATE TO THE PRODUCT WILL NOT MATERIALLY REDUCE OR DEGRADE SUCH PRODUCTS OVERALL FUNCTIONALITY.

1. DEFINITIONS

1.1 "Affiliate" means, with respect to each party, an entity that controls, is controlled by, or is under common control with such party. For the purposes of this definition, "control" means the beneficial ownership of more than fifty percent (50%) of the voting power or equity in an entity.

1.2 "Beta Product" means any Product (or portion of a Product) that Sophos identifies as beta, pre-release, early access, or preview, and that is made available to Customer during the Subscription Term but not made generally available for use.

1.3 "Cloud Service" means the hosted software-as-a-service offering or other cloud-enabled feature of the Software.

1.4 "Confidential Information" means any non-public, confidential, or proprietary information of the disclosing party that is clearly marked confidential or reasonably should be assumed to be confidential given the nature of the information and the circumstances of disclosure, including any Beta Products and related Documentation.

1.5 "Customer" means the company or legal entity identified in the applicable Schedule, or in the event there is no applicable Schedule, "Customer" means: (a) the company or legal entity on whose behalf a User accesses or uses the Service, or (b) an individual who accesses or uses the Service on such individual's own behalf.

1.6 "Customer Content" means all software, data (including Personal Data), non-Sophos or third-party applications, and any other content, communications or material, in any format, and any system, network, or infrastructure provided or made accessible by Customer or User to Sophos in connection with Customer's access and use of the Product.

1.7 "Documentation" means any technical specifications, online help content, user manuals, or similar materials pertaining to the implementation, operation, access, and use of the Product that are made available by Sophos, as may be revised by Sophos from time to time.

1.8 "Entitlement" means the quantity of units of the Product that Customer has purchased and the associated Subscription Term, each as set forth on the applicable Schedule.

1.9 "Fixes" means any custom or sample code, files, or scripts provided by Sophos as part of the provision of technical support for Hardware or Product that do not form part of Sophos's standard offerings.

1.10 "Hardware" means any Sophos appliance or physical computing components (whether new or refurbished, and whether or not subject to payment of a fee) on which the Software operates, and any related components or

peripherals (including, but not limited to, power cords, fans, power supply modules, drives, carries, ship kits, and rack mount kits).

1.11 “Managed Service” means any managed security services or other associated security services for which the Service Description is published with this Agreement at https://www.sophos.com/en-us/legal.

1.12 “Partner” means Sophos authorized reseller, distributor, or other independent third party from which Customer purchases a subscription to the Product.

1.13 “Personal Data” means any information relating to an identified or identifiable individual or that is otherwise defined as “personal data”, “personal information”, or “personally identifiable information” under applicable data protection laws.

1.14 “Product” means Software, Service, Service Software, Trial Product, or Beta Product that Customer is authorized to access and use under the terms of this Agreement (and any data generated by them, excluding Customer Content), including any applicable support and maintenance services, Documentation, and any Fixes.

1.15 “Sanctions and Export Control Laws” means any law, regulation, statute, prohibition, or similar measure applicable to the Product and/or to either party relating to the adoption, application, implementation, and enforcement of economic sanctions, export controls, trade embargoes, or any other restrictive measures, including, but not limited to, those administered and enforced by the European Union, the United Kingdom, and the United States, which shall be considered applicable to the Product.

1.16 “Schedule” means the order confirmation issued by Sophos, or other equivalent documentation, that details Customer’s purchase of a Product and the Entitlement, and may include other access and use details for the Product.

1.17 “Service” means a Managed Service or Cloud Service that Customer is authorized to access and use under the terms of this Agreement.

1.18 “Service Description” means Sophos’s description of a Security Service’s features, including any additional Service-specific terms and requirements, available at https://www.sophos.com/en-us/legal.aspx.

1.19 “Service Software” means any Software made available by Sophos for Customer’s use in connection with a Service.

1.20 “Software” means Sophos computer programs including updates, upgrades, firmware, including any software embedded in Hardware, and applicable Documentation.

1.21 “Sophos Materials” means (i) all Sophos proprietary materials, any written or printed summaries, analyses or reports generated in connection with a Product, including written reports that are created for Customer in the course of providing a Service, and (ii) data generated by Sophos in connection with Customer’s use of a Product, including but not limited to, detections, threat data, indicators of compromise, and any contextual data (but excluding Customer Content).

1.22 “Subscription Term” means the term of Customer’s authorized access and use of the Product, as set forth in the applicable Schedule.

1.23 “Third Party Services” has the meaning set forth in Section 3.3 below.

1.24 “Threat Intelligence Data” means any information about malware, threats, actual or attempted security events, including but not limited to their frequency, source, associated code, general identifiers, attacked sectors, and geographies.

1.25 “Trial Product” has the meaning set forth in Section 2.4(a) below.

1.26 “Trial Term” has the meaning set forth in Section 2.4(a) below.

1.27 “Usage Data” means any diagnostic and usage-related information from the use, performance and operation of the Product, including, but not limited to, type of browser, Product features, and systems that are used and/or accessed, and system and Product performance-related data.

1.28 “Use Level” has the meaning set forth in Section 2.2 below.

1.29 “User” means Customer’s and its permitted Affiliates’ employees, contractors, and similar personnel authorized by Customer or its Affiliates to access and use the Product on such entity’s behalf.

2. PRODUCT USE AND RESTRICTIONS

2.1 License and Right to Access and Use. Subject to Customer’s compliance with the terms of this Agreement, Sophos grants Customer a non-exclusive, non-transferable, worldwide license and right to access and use the Product listed in the Schedule during the applicable Subscription Term solely for Customer’s internal information security purposes, except that Customers may use Sophos Factory for Customer’s internal business purposes. Customer may permit its Affiliates and Users to use the Product in accordance with this Agreement, provided that Customer remains fully responsible and liable for their use of the Product and compliance with the terms and conditions of this Agreement. Customer may make a reasonable number of copies of the Software for backup or disaster recovery purposes. Additionally, during the Agreement term, Sophos grants to Customer a limited, non-exclusive license to use such Sophos Materials solely and for Customer’s own internal information security purposes only.

2.2 Use Level. The Entitlement together with the defined Product unit(s) or meter(s) specified in the Licensing Guidelines at https://www.sophosExhibit.com/en-us/legal.aspx and attached hereto for reference as **Exhibit A** form the applicable Customer access and use level (“Use Level”). Customer may access and use the Product in accordance with the applicable Use Level, and may not exceed the Use Level at any time. Customer’s use and access of the Product in excess of its Entitlement may result in degraded, incomplete or failed Service delivery. If Customer wishes to increase its Use Level, it must first purchase the corresponding additional Entitlement. If Customer exceeds its Use Level, Customer will pay any invoice for such excess use issued by Sophos or a Partner in accordance with Section 6.

2.3 Restrictions. Except as specifically permitted in this Agreement, Customer will not (and will not allow an Affiliate, User, or third party to), directly or indirectly: (a) sublicense, resell, rent, lease, distribute, market, commercialize, or otherwise transfer rights to, or usage of, all or any portion of the Product, or provide the Product on a timesharing, service bureau, or other similar basis; (b) modify, copy, adapt, translate, create derivative works of, reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of, any part of the Product, except when expressly permitted by law and when essential to achieve interoperability of the Software with another software program; (c) remove, alter, or obscure any proprietary rights notices contained in or affixed to the Product; (d) attempt to gain unauthorized access to the Product; (e) attempt to disrupt, degrade, impair, or violate the integrity, security, or performance of the Product, including, without limitation, by executing any form of network monitoring; (f) use the Product to store, transmit, or propagate any viruses, software routines, or other code designed to permit unauthorized access, to disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (g) upload any content to Product that is unlawful, pornographic, obscene, indecent, harassing, racially or ethnically offensive, harmful, threatening, discriminatory, defamatory, or facilitates or promotes illegal activities; (h) take any action that imposes or may impose an unreasonable or disproportionately large load on Sophos’s infrastructure, as determined by Sophos in its sole discretion; (i) disable or circumvent any monitoring or billing mechanism related to the Product; (j) use any feature of Sophos APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (k) access or use the Product in a manner that violates applicable law or regulation, infringes third party rights, or violates the terms and conditions of this Agreement.

2.4 Trial Products, Beta Products, Free Products and Fixes.

(a) If Sophos permits Customer to conduct a free trial or evaluation of a Product ("Trial Product"), Customer may access and use the Trial Product for thirty (30) days, or such other duration specified by Sophos in writing ("Trial Term").

(b) From time to time, Sophos may invite Customer to try a Beta Product, for a period specified by Sophos and at no charge, which Customer may accept or decline in Customer's sole discretion. Customer will comply with testing guidelines that Sophos provides in connection with Customer's access and use of a Beta Product and will make reasonable efforts to provide Feedback in accordance with Section 5.3. Sophos may discontinue a Beta Product at any time in its sole discretion and may not make it generally available.

(c) Trial Products and Beta Products are provided for internal testing and evaluation solely for Customer's own internal information security purposes.

(d) Sophos may make certain Products, portions of certain Products, or certain usage tiers available free of charge ("Free Product"). Customer's right to access and use Free Product is not guaranteed for any period of time and Sophos reserves the right, in its sole discretion, to: (i) limit or terminate Customer's use of Free Product; or (ii) reduce, change, or deprecate the functionality of Free Product. For Free Product, only community support is available via https://community.sophos.com. Sophos may make certain Products available for personal use ("Home Use License"). Customer may only use Products made available under Home Use License for their own non-commercial personal use and not for any other purposes. Fixes may only be used in conjunction with the Hardware or Product for which such Fixes were developed.

(e) TRIAL PRODUCTS, BETA PRODUCTS, FREE PRODUCTS, HOME USE LICENSES AND FIXES ARE PROVIDED "AS IS" WITHOUT ANY SUPPORT, INDEMNITY, LIABILITY OR REMEDY OF ANY KIND. TO THE EXTENT ALLOWED BY APPLICABLE LAW, SOPHOS EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY, CONDITION, OR OTHER IMPLIED TERM AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF TRIAL PRODUCTS, BETA PRODUCTS, FREE PRODUCTS, HOME USE LICENSES OR FIXES.

(f) The terms of this Section 2.4 apply, and prevail over any conflicting terms in this Agreement, with respect to all access to and use of Trial Products, Beta Products, Free Products, Home Use Licenses or Fixes.

2.5 Modifications to Product. Sophos may in its sole discretion modify or update the Product from time to time without materially reducing or degrading its overall functionality.

2.6 Support. Sophos will provide the technical support specified in the applicable Schedule or documentation during the Subscription Term. Additional technical support packages may be available for an additional fee. Technical support packages are described at: https://www.sophos.com/en-us/support/technical-support.aspx. From time to time, Sophos performs scheduled maintenance to update the servers, software, and other technology that are used to provide the Service and will use commercially reasonable efforts to provide prior notice of such scheduled maintenance. Customer acknowledges that, in certain situations, Sophos may need to perform emergency maintenance of the Service without providing prior notice.

2.7 Open Source. The Product may contain open source software that are made available under applicable open source license agreements. This Agreement does not alter any rights or obligations Customer may have under the applicable open source licenses. Any open source software that is delivered as part of the Product and which may not be removed or used separately from the Product is covered by the warranty, support and indemnification provisions applicable to the Product.

2.8 Hardware. The use of Hardware is governed by this Agreement, as modified by the Sophos Hardware Terms available at https://sophos.com/legal/hardware-terms and attached hereto as **Exhibit B** for reference. In the event of any conflict between the Hardware Terms and this Agreement, the Hardware Terms will take precedence.

3. CUSTOMER OBLIGATIONS

3.1 Access and Use. Customer is solely responsible for: (a) accessing and using the Product in accordance with the Documentation; (b) determining the suitability of the Product for Customer's internal information security purposes; (c) configuring the Product appropriately; (d) complying with any regulations and laws (including, without limitation, export, data protection, and privacy laws) applicable to Customer Content and Customer's use of the Product; (e) Customer's and Users' access and use of the Product; (f) all activity occurring under Customer's Product and support accounts, including the rights and privileges Customer grants to Users and any activity undertaken or decision made by Users regarding Product delivery and usage; (g) providing all reasonable information and assistance required for Sophos to deliver the Product, or enable Customer's or Users' access and use of the Product; (h) using reasonable means to protect the account information and access credentials (including passwords and devices, or information used for multi-factor authentication purposes) used by Customer and Users to access the Product; and (i) promptly notifying Sophos of any unauthorized account use or other suspected security breach, or unauthorized use, copying, or distribution of the Product or Customer Content.

3.2 Accuracy of Information. Customer agrees to provide complete and accurate Customer and User identification information in connection with access to and use of the Product, including but not limited to providing reasonable Customer and User contact details and information upon Sophos's or Partner's request.

3.3 Third Party Services. The Product may enable or require Customer to associate its Product 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 Product, and Sophos does not control and is not responsible for the Third Party Services. Customer is solely responsible for: (a) obtaining and complying with any terms of access and use of the Third Party Services, including any separate fees or charges imposed by the provider of the Third Party Services; and (b) configuring the Third Party Services appropriately. Sophos disclaims all responsibility and liability arising from or related to Customer's access or use of the Third Party Services, including any impact on Product capabilities as a result of Customer's use of, or reliance upon, the Third Party Services.

3.4 Critical Applications. The Product is not fault tolerant and use of the Product is not recommended in or in association with safety critical applications where the failure of the Products to perform can reasonably be expected to result in death, personal injury, loss of property, or severe physical or environmental damage. Any use contrary to this disclaimer is at Customer's own risk and Sophos is not liable for such use.

4. CUSTOMER CONTENT; PROTECTION OF CUSTOMER CONTENT; CONFIDENTIALITY; USE OF DATA

4.1 Customer Content. Customer is solely responsible for all Customer Content, including but not limited to its accuracy, quality, and legality. Customer represents and warrants that it: (a) has the legal rights to provide Customer Content to Sophos or/and to other users of the Product as applicable; (b) has provided any required notices and has obtained any consents and/or authorizations (including any required from Users) related to its access and use of the Product and the processing of and access to Customer Content by Sophos; and (c) will comply with all applicable laws and regulations for collecting and processing Customer Content, and transferring Customer Content to Sophos. Customer is responsible for taking and maintaining appropriate steps to protect the confidentiality, integrity, and security of Customer Content, including but not limited to: (i) controlling access that Customer provides to Users; and (ii) backing up Customer Content. In some cases, Sophos may make certain Sophos consumer products available to Customer for personal use by users associated with Customer's organization or institution, and in such cases, Customer agrees that Customer is solely responsible for: (1) providing any required notices and (2) obtaining necessary consents and/or authorizations related to the access/use of the consumer products by the users and the processing of and access to users' information by Sophos.

4.2 Use of Customer Content by Sophos. Customer grants Sophos a non-exclusive, worldwide, royalty-free license to access and use the Customer Content to perform its obligations and exercise its rights under this Agreement.

4.3 Protection and Processing of Customer Content by Sophos. Sophos will maintain appropriate administrative, physical, and technical measures designed to protect the security, confidentiality, and integrity of Customer Content processed by Sophos. The Data Processing Addendum ("DPA") located at https://www.sophos.com/en-us/legal/data-processing-addendum.aspx and attached hereto as **Exhibit C** for reference is incorporated by reference into this Agreement if the provision of Product constitutes any "processing" by Sophos of any "personal data" within the Customer Content, but only to the extent such processing falls within the scope of "Applicable Data Protection Laws" (each term as defined in the DPA). In the event of any conflict between the terms of the DPA and this Agreement, the terms of the DPA will take precedence.

4.4 Content Restrictions. If Customer's access and use of the Product requires Customer to comply with industry-specific data security or data protection obligations, Customer will be solely responsible for such compliance. Customer may not use the Product in a way that would subject Sophos to those industry-specific regulations without obtaining Sophos' prior written agreement.

4.5 Confidentiality.

(a) Each party acknowledges that it and its Affiliates ("Receiving Party") may have access to Confidential Information of the other party and its Affiliates ("Disclosing Party") in connection with this Agreement. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but not less than reasonable care). The Receiving Party agrees to (i) not use any Confidential Information for any purpose other than to perform its obligations and exercise its rights under this Agreement, and (ii) restrict dissemination of Confidential Information only to individuals or third parties with a "need to know" such information and who are under a substantially similar duty of confidentiality. A Receiving Party may disclose the Disclosing Party's Confidential Information in any legal proceeding or as required as a matter of applicable law or regulation (such as in response to a subpoena, warrant, court order, governmental request, or other legal process); provided, however, that to the extent permitted by applicable law, the Receiving Party will (1) promptly notify the Disclosing Party before disclosing the Disclosing Party's Confidential Information; (2) reasonably cooperate with and assist the Disclosing Party, at the Disclosing Party's expense, in any efforts by the Disclosing Party to contest the disclosure; and (3) disclose only that portion of the Disclosing Party's Confidential Information that is legally required to be disclosed.

(b) Notwithstanding the above, a Disclosing Party's Confidential Information will not include information that: (i) is or becomes a part of the public domain through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure by the Disclosing Party and had not been obtained by the Receiving Party either directly or indirectly from the Disclosing Party; (iii) is lawfully disclosed to the Receiving Party by a third party without restriction on the disclosure; or (iv) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information. Sophos recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by Sophos.

4.6 Usage Data and Threat Intelligence Data. Sophos may collect, access, use, process, transmit, or store Usage Data and Threat Intelligence Data for: (a) product improvement; (b) research and development purposes; and (c) deriving statistical data using information that is aggregated, anonymized, de-identified, or otherwise rendered not reasonably associated or linked to an identifiable individual or to Customer or Users ("Statistical Data"). Sophos retains all intellectual property rights in such Statistical Data. Sophos may share Threat Intelligence Data (including from Customer Content, if it is anonymized, de-identified, or otherwise rendered not reasonably associated or linked to an identifiable individual or Users) with selected reputable members of the IT industry for the purposes of promoting awareness of security risks, and anti-spam and security threat research.

5. OWNERSHIP RIGHTS

5.1 Customer Ownership. Except as expressly provided otherwise in this Agreement, as between Sophos and Customer, Customer retains all right, title, and interest in and to Customer Content.

5.2 Sophos Ownership. As between Sophos and Customer, Sophos retains all right, title, and interest, including all intellectual property rights, in and to the Product and Sophos Materials, including all improvements, enhancements, modifications, derivative works, logos, and trademarks. Sophos reserves all rights in and to the Product that are not expressly granted under this Agreement.

5.3 Feedback. Customer or Users may provide suggestions, enhancement or feature requests, or other feedback to Sophos with respect to the Product ("Feedback"). If Customer provides Feedback, Sophos may use the Feedback without restriction and without paying any compensation to Customer, and Customer hereby irrevocably assigns to Sophos all intellectual property rights in and to such Feedback.

6. FEES, PAYMENT AND TAXES

If Customer is purchasing a subscription to the Product from a Partner, all provisions related to fees, taxes, and payment terms will be exclusively between the Partner and Customer. Otherwise, Customer will pay Sophos, or the local Sophos sales Affiliate, the fees for the Product within thirty (30) days of the invoice receipt date (in the currency and via the payment method specified on the invoice), unless otherwise noted in the applicable invoice. If permitted by applicable law, any delay in making payment shall entitle Sophos to charge interest on the overdue payment at the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. Vendor shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

7. WARRANTIES; DISCLAIMERS; LIMITATION OF LIABILITY

7.1 Warranties. Each party warrants to the other party that it has the requisite authority to enter into this Agreement. Sophos warrants that: (a) for a period of ninety (90) days from the purchase date the Software will perform substantially in accordance with the Documentation; and (b) during the Subscription Term, it will provide the Services using commercially reasonable skill and care, and the Services will materially conform to the corresponding Documentation. Customer's sole and exclusive remedy for Sophos's breach of the foregoing warranty is, at Sophos's option, either (i) repair or replacement of the Product, or (ii) a pro rata refund of the fees paid to Sophos or a Partner for the period in which Sophos was in breach of the foregoing warranty. This warranty is conditioned upon Customer providing Sophos prompt written notice of the Product's non-conformity, and using the Product in compliance with this Agreement and in accordance with the Documentation. Where Sophos provides a refund of fees paid for Software, Customer must return or destroy all copies of the applicable Software.

7.2 Warranty Disclaimer. EXCEPT AS EXPRESSLY STATED IN SECTION 7.1, TO THE EXTENT ALLOWED BY APPLICABLE LAW, SOPHOS AND ITS THIRD-PARTY LICENSORS AND SUPPLIERS EXPRESSLY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY, CONDITION, OR OTHER IMPLIED TERM AS TO MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THE PRODUCT. SOPHOS MAKES NO WARRANTY OR REPRESENTATION THAT THE PRODUCT: (A) WILL BE UNINTERRUPTED, COMPLETELY SECURE, ERROR-FREE, FAILSAFE, OR FREE OF VIRUSES; (B) WILL MEET CUSTOMER'S BUSINESS REQUIREMENTS OR OPERATE WITH CUSTOMER'S CURRENT SYSTEMS; OR (C) WILL IDENTIFY OR REMEDIATE ALL THREATS OR INDICATORS OF COMPROMISE. SOPHOS IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION, OR SECURITY OF THE PRODUCT THAT MAY ARISE FROM CUSTOMER CONTENT, THIRD PARTY SERVICES, OR ANY OTHER SERVICES PROVIDED BY THIRD PARTIES. SOPHOS DISCLAIMS ANY RESPONSIBILITY OR LIABILITY FOR ANY INTERCEPTION OR INTERRUPTION OF ANY COMMUNICATIONS THROUGH THE INTERNET, NETWORKS, OR SYSTEMS OUTSIDE SOPHOS'S CONTROL.

7.3 Limitation of Liability.

IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, CONSEQUENTAL, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES, OR ANY LOSS OF REVENUES, BUSINESS, PROFITS (IN EACH CASE WHETHER DIRECT OR INDIRECT), OR DATA LOSS OR CORRUPTION IN CONNECTION WITH THIS AGREEMENT OR THE PRODUCT, EVEN IF THE DAMAGES WERE FORESEEABLE OR A PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

IN NO EVENT WILL THE AGGREGATE LIABILITY OF SOPHOS OR ITS AFFILIATES FOR DIRECT DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCT EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY CUSTOMER TO SOPHOS OR THE PARTNER, AS APPLICABLE, UNDER THIS AGREEMENT DURING THE APPLICABLE SUBSCRIPTION TERM.

THE LIMITATION OF LIABILITY HEREIN WILL NOT APPLY TO LIABILITY ARISING FROM A PARTY'S INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, INDEMNIFICATION OBLIGATIONS, OR THE FRAUD, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY.

THE LIMITATIONS AND EXCLUSIONS OF LIABILITY IN THIS SECTION 7.3 APPLY (A) WHETHER SUCH CLAIMS ARISE UNDER CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY, STATUTE, OR OTHERWISE, AND (B) NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY. NOTHING IN THIS AGREEMENT LIMITS OR EXCLUDES ANY LIABILITY WHICH CANNOT BE LIMITED OR EXCLUDED UNDER ANY APPLICABLE LAW. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PHYSICAL INJURY, TANGIBLE PROPERTY DAMAGE OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

8. INDEMNIFICATION

8.1 Indemnification by Sophos.

(a) Sophos will (i) indemnify, have the right to intervene to defend, and hold Customer harmless from any third party claim, action, suit, or proceeding alleging that Customer's access and use of the Product in accordance with this Agreement infringes such third party's patent, trademark, or copyright; and (ii) reimburse Customers' reasonable attorney's fees and costs actually incurred and any damages finally awarded against Customer by a court of competent jurisdiction or agreed to by Sophos in a settlement. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. If a third-party claim is made or appears likely to be made, Sophos, in its sole discretion, may: (1) procure the right for Customer to continue accessing or using the Product under the terms of this Agreement; or (2) modify or replace the Product to be non-infringing without material decrease in functionality. If Sophos, in its sole discretion, determines that neither of the foregoing options is reasonably feasible, Sophos may terminate the Customer's license to or right to use the Product upon written notice to Customer, and provide or authorize a pro rata refund of the fees paid by Customer to Sophos or the Partner, respectively, for the remainder of the applicable Subscription Term. The foregoing shall be Sophos's entire obligation and Customer's exclusive remedy regarding any third-party claim against Customer.

(b) Sophos will have no indemnity obligation for any claim to the extent such claim, in whole or in part, is based on: (i) a modification of the Product by Customer or a third party; (ii) access or use of the Product in a manner that violates the terms and conditions of this Agreement; (iii) technology, designs, instructions, or requirements provided by Customer or a third party on Customer's behalf; (iv) combination, operation, or use of the Product with non-Sophos products, software, services, or business processes, if a claim would not have occurred but for such combination, operation, or use; or (v) Customer Content or Third Party Services.

8.2Reserved.

8.3 Indemnification Procedures. The indemnified party ("Indemnitee") will: (a) promptly notify the indemnifying party ("Indemnitor") in writing of any indemnifiable claim; (b) give Indemnitor all reasonable assistance, at Indemnitor's expense; and (c) give Indemnitor sole control of the defense and settlement of the claim. Any

settlement of a claim will not include a specific performance obligation other than the obligation to cease using the Product, or an admission of liability by the Indemnitee, without the Indemnitee's consent. The Indemnitee may join in the defense of an indemnifiable claim with counsel of its choice and at its own expense.

9. TERM AND TERMINATION

9.1 Term. This Agreement will remain in effect until the expiration of the applicable Subscription Term, unless earlier terminated pursuant to this Section 9.2.

9.2 Agreement Termination and Service Suspension When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Sophos shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Sophos may immediately and temporarily suspend Customer's or User's access and use of the Service, or portions of the Service, if Sophos believes there is a significant threat to the functionality, security, integrity, or availability of the Service to Customer or to other customers. When reasonably practicable and lawfully permitted, Sophos will provide Customer with advance notice of any such Service suspension. Sophos will use reasonable efforts to re-establish the Service promptly after it determines that the issue causing the suspension has been resolved. Any Service suspension under this Section shall not excuse Customer's payment obligations under this Agreement.

9.3 Effect of Termination. Upon termination or expiration of this Agreement: (a) all Customer rights under this Agreement relating to the Product will immediately terminate; (b) Customer is no longer authorized to access the Product or Customer's account; and (c) Customer must destroy any copies of the Product within Customer's control. Upon any termination by Customer for Sophos's uncured material breach of the Agreement, Sophos will provide or authorize a pro rata refund of the fees paid by Customer to Sophos or the Partner, respectively, for the remainder of the applicable Subscription Term. Upon any termination by Sophos for Customer's uncured material breach of the Agreement, Customer will pay any unpaid fees covering the remainder of the then-current Subscription Term.

9.4 Customer Content upon Termination. After termination or expiration of this Agreement, Customer shall have thirty (30) days from the termination date to retrieve data, after which Customer agrees that Sophos has no obligation to Customer to retain Customer Content, which may thereafter be permanently deleted by Sophos. Sophos will protect the confidentiality of Customer Content residing in the Service for as long as such information resides in the Service.

9.5 End-of-Life. Customer's right to use the Product, and any features of the Product, is subject to the end-of-life policy available at https://www.sophos.com/en-us/content/product-lifecycle.aspx. Customer acknowledges and agrees that it is Customer's sole responsibility to review the end-of-life policy for each Product.

10. EXPORT CONTROL; COMPLIANCE WITH LAWS

10.1 Export Compliance. Customer is solely responsible for ensuring that the Product is used, accessed, and disclosed in compliance with Sanctions and Export Control Laws. Customer certifies that Customer or Users, or any party that owns or controls Customer or Users, are not (a) ordinarily resident in, located in, or organized under the laws of any country or region subject to economic or financial trade sanctions or trade embargoes imposed, administered, or enforced by the European Union, the United Kingdom, or the United States; (b) an individual or entity on the Consolidated List of Persons, Groups, and Entities Subject to European Union Financial Sanctions; the U.S. Department of the Treasury's List of Specially Designated Nationals and Blocked Persons or Foreign Sanctions Evaders List; the U.S. Department of Commerce's Denied Persons List or Entity List; or any other sanctions or restricted persons lists maintained by the European Union, the United Kingdom, or the United States; or (c) the target or subject of any Sanctions and Export Laws. Customer further certifies that it and Users will not, directly or indirectly, export, re-export, transfer, or otherwise make available (i) the Product, or (ii) any data, information, software programs, and/or materials resulting from the Product (or direct product thereof) to any person described in (a) through (c) or in violation of, or for any purpose prohibited by, Sanctions and Export Control Laws, including for proliferation-related end uses. Customer agrees that Sophos has no obligation to provide the Product where Sophos

believes the provision of the Product could violate Sanctions and Export Control Laws. Further details are available at https://www.sophos.com/en-us/legal/export.aspx.

10.2 Compliance with Laws. Each party agrees to comply with all laws applicable to the actions and obligations contemplated by this Agreement. Each party warrants that, during the term of this Agreement, neither party nor any of its officers, employees, agents, representatives, contractors, intermediaries, or any other person or entity acting on its behalf has taken or will take any action, directly or indirectly, that contravenes (a) the United Kingdom Bribery Act 2010, (b) the United States Foreign Corrupt Practices Act 1977, or (c) any other applicable anti-bribery laws or regulations anywhere in the world.

11.GENERAL

11.1 Assignment. Customer may not sublicense, assign, or transfer its rights or obligations under this Agreement without Sophos's prior written consent. Sophos may in its sole discretion assign, novate, subcontract, or otherwise transfer any of its rights or obligations hereunder.

11.2 Notice. Sophos may provide Customer with notice (a) if applicable to the Product, by means of a general notice on the Product portal, on the Sophos.com website, or any other website used as part of the Product, and (b) if specific to the Customer, by electronic mail to the e-mail address in Sophos's records. All notices to Sophos concerning this Agreement will be addressed to The Legal Department, Sophos Limited, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, United Kingdom with a copy to legalnotices@sophos.com.

11.3 Waiver & Severability. Failure by either party to enforce any term or condition of this Agreement will not be construed as a waiver of any of its rights under it. If any provision of the Agreement is held to be invalid or unenforceable, the remaining provisions of the Agreement will remain in force to the fullest extent permitted by law.

11.4 Force Majeure. In accordance with GSAR 552.212-4(f), except for payment obligations, neither party will be liable to the other for any delay or failure to perform hereunder due to circumstances beyond such party's reasonable control.

11.5 Community Forum. Customer and other Sophos customers may exchange ideas and technical insight related to Sophos offerings in the Sophos Community site at https://community.sophos.com/. Sophos does not endorse, warrant, or guarantee any information posted on that site, and Customer alone assumes the risk of using any such information.

11.6 Third Party Flow-down. If the Product is Sophos Central Wireless, the Google Maps / Google Earth Additional Terms of Service (including the Google Privacy Policy) apply to use of the Product. If the Product utilizes the Talos Rules, Cisco Inc. is a third-party beneficiary to this Agreement with regards to Customer's use of the Talos Rules.

11.7 Service Monitoring. Customer acknowledges that Sophos continuously monitors the Service to: (a) track usage and Entitlement, (b) provide support, (c) monitor the performance, integrity, and stability of the Service's infrastructure, (d) prevent or remediate technical issues, and (e) detect and address illegal acts or violations of Section 2.3 (Restrictions).

11.8 Audit Rights. To the extent tracking of Customer's Use Level (Section 2.2) is not possible, Sophos may audit Customer's use of the Product to verify that Customer's usage complies with the applicable Entitlement, including without limitation through self-certifications, on-site audits and/or audits done using a third party auditor. An audit will be done upon reasonable notice and during normal business hours, but not more often than once each year unless a material discrepancy was identified during the course of a prior review. Customer further agrees to keep accurate records sufficient to certify Customer's compliance with this Agreement, and, upon Sophos's request, Customer will promptly provide the necessary details certifying Customer's aggregate usage of the Product. Sophos will bear the costs of any such audit (other than Customer's costs associated with any self-certification). If an audit reveals that Customer has used in excess of its purchased Entitlement, Customer shall promptly pay: (i) the additional fees to reflect the Customer's actual entitlement usage, and (ii) any past excess usage shown in the report.

11.9 United States Government Users; Non-Waiver of Government Immunity.

(a) The Product and Documentation are considered “commercial computer software” and “commercial computer software documentation” for the purposes of FAR 12.212 and DFARS 227.7202, as amended, or equivalent provisions of agencies that are exempt from the FAR or that are U.S. state or local government agencies. Any use, modification, reproduction, release, performance, display, or disclosure of the Product by the U.S. Government and U.S. state and local government agencies will be governed solely by this Agreement, and except as otherwise explicitly stated in this Agreement, all provisions of this Agreement shall apply to the U.S. Government and U.S. state and local government agencies.

(b) If Customer is a federal, state, or other governmental instrumentality, organization, agency, institution, or subdivision, the limitations of liability and Customer’s indemnity obligations herein shall apply only in the manner and to the extent permitted by applicable law, and without waiver of Customer’s constitutional, statutory, or other immunities, if any.

11.10 Governing Law and Jurisdiction. This Agreement shall be governed by and construed in accordance with the Federal laws of the United States . The parties agree that the UN Convention on Contracts for the International Sale of Goods (CISG, Vienna, 1980) shall not apply to this Agreement.

11.11 Survival. The following sections, together with any other terms necessary for the interpretation or enforcement of this Agreement, will survive termination or expiration of this Agreement: 1 (Definitions), 4.5 (Confidentiality) for five (5) years, 4.6 (Usage Data and Threat Intelligence Data), 5 (Ownership Rights), 6 (Fees, Payment and Taxes), 7 (Warranties; Disclaimers; Limitation of Liability), 8 (Indemnification), 9.3 (Effect of Termination), 9.4 (Customer Content upon Termination), and 11 (General).

11.12 Independent Parties. Sophos and Customer are independent contractors, and nothing in this Agreement will create a partnership, joint venture, agency, franchise, sales representative, or employment relationship between the parties.

11.13 Entire Agreement. This Agreement, the Service Description (where applicable), the Schedule, the Licensing Guidelines, and the documents and policies referenced herein constitute the entire agreement between the parties with respect to the Product and supersede all prior or contemporaneous oral or written communications, agreements or representations with respect to the Product. The Service Description is incorporated by reference into this Agreement if Customer’s purchase and use of the Service is described in the Service Description. The parties agree that Sophos uses the attached terms and the non-materially updated version that is posted online through embedded URLs and hyperlinks shall prevail, including but not limited to any updates to the applicable terms or descriptions taking effect upon posting. Any modification to the terms and conditions of this Agreement shall require a written amendment to this Agreement signed by authorized representatives of both parties. If there are any inconsistencies between the English language version of this Agreement and any translated version, the English language version shall prevail.

These End Customer Terms of Use will apply to Sophos Products used by the Customer.

Exhibit A

Licensing Guidelines

This document forms part of the Sophos End User Terms of Use attached hereto and available at https://www.sophos.com/en-us/legal, or other written agreement governing access and use of Sophos products and services. Capitalized terms not separately defined in these Licensing Guidelines have the same meanings as in the Sophos End User Terms of Use, or other written agreement, as applicable. Please refer to this archived Licensing Guidelines for any entitlements that were acquired or renewed before January 17, 2022.

Sophos Products are licensed or made available by the applicable units specified in the table below. The Schedule issued by Sophos specifies the number of applicable units that the Customer has ordered for each Product.

Sophos reserves the right to non-materially change or update these Licensing Guidelines at any time and the updated Licensing Guidelines will be effective when posted on the website.

The following definitions apply to the table below:

Definitions for Sophos Products

1.'Computer' means any device or computing environment which benefits from the Product (for example, but without limitation, workstations, personal computers, laptops, netbooks, tablets, smartphones, and environments connected to an email server, an internet proxy or a gateway device, or a database). The Product does not have to be physically installed on the computer environment to provide benefit, nor is there a requirement for the computing hardware to be owned by the Customer. The term Computer as defined herein includes, without limitation, non-persistent deployments, electronic devices that are capable of retrieving data, and virtual machines.

2. 'Server' means a Computer (i) upon which the Product is installed or (ii) which benefits from the Product, wherein the Computer provides at least one application, client service, or capability.

3. 'User' means an employee, consultant or other individual who benefits from the Product.
NOTE: The Product does not have to be physically installed on the User's computer environment in order to provide benefit to the User.

4. 'Cloud Asset' means a single virtual machine instance (including any server instance or database instance) or container image, within a Cloud Environment that benefits from, or whose configuration is accessed by, the Product. For the purposes of this definition, ‘Cloud Environment’ means an environment facilitating or involved in the delivery of computing services over the internet, including but not limited to Amazon Web Services (AWS) accounts, Microsoft Azure subscriptions, Google Cloud Platform (GCP) projects, Kubernetes clusters, development code repositories, and container registries.

Terms for Products

General exception for Education, Health and Government Entities:
If Licensee or Customer is an educational, health or government entity, Products or Services that are usually licensed or made available on a per User basis may alternatively, at Sophos’ option, be licensed or made available on a per Computer basis, or for email Products only, on a per mailbox basis. If a bundle includes both email and non-email Products, the aforementioned licenses must be the higher of the entity’s Computer and mailbox count. If Licensee subsequently transfers such Products or Services to an entity that does not fall within the education, health or government sector then the License Entitlement or Service Entitlement shall revert to calculation on a per User basis.

Number of Computers (Devices) per User:

In the case of Products licensed or made available by User, each User may use a reasonable number of Computers unless a specific cap on Computers per User is stated in the table below. Sophos reserves the right to apply a cap on Computers where usage is deemed unreasonable.

TRIAL/EVALUATION LICENSES

Where permitted, Customer may request a "trial" license or subscription of a commercially available Product for evaluation purposes. In some cases, "evaluation" licenses or subscriptions may be generated automatically by Sophos, in its sole discretion, for Customers of Sophos Central Endpoint Protection and Server Protection Products; for example, in order to enable testing of pre-release features and Products, and/or for applicable temporary license or subscription extensions.

All such trial/evaluation licenses and subscriptions, whether or not they are labelled as such, are governed by the terms of the Sophos End User Terms of Use, or other written agreement (as applicable) relating to trials/evaluations; are provided for temporary usage only; and may be used for no longer than thirty (30) days unless otherwise specified by Sophos in writing. Note: a non-applicable date of "December 31, 2999" may be displayed in the Sophos Central console for evaluation licenses or subscriptions that are generated by Sophos.

Sophos Product	Licensing Model	Applicable Unit(s)	NOTES.EXCEPTIONS AND APPLICABLE LIMITS
Sophos Central Products			
Cloud Optix Advanced	Subscription	Cloud Assets	A subscription includes a maximum number of Cloud Assets. The following Data Lake use limitations apply: • 1MB daily storage per Cloud Asset with a maximum 90 days storage
Central Intercept X Advanced for Server with XDR	Subscription	per Server	Following Data Lake usage limitations apply: • 40MB daily storage with a maximum 90 days storage per subscription; and • 1,000 daily Data Lake API queries.
Central Intercept X Advanced for Server	Subscription	per Server	N/A
Central Intercept X Essentials for Server	Subscription	per Server	N/A
Sophos Capsule8 Protect	Subscription	per Server	N/A
Sophos Capsule8 Protect+	Subscription	per Server	N/A
Sophos Capsule8 Complete	Subscription	per Server	N/A
Central Intercept X Advanced with XDR	Subscription	per User	Following Data Lake usage limitations apply: • 20MB daily storage with a maximum 90 days storage per subscription; and • 1,000 daily Data Lake API queries.
Central Intercept X Advanced	Subscription	per User	N/A
Central Endpoint Intercept X	Subscription	per User	N/A
Central Intercept X Essentials	Subscription	per User	N/A
Central Mobile Advanced	Subscription	per User	Maximum upload size: 25 MB for documents, 300 MB for apps
Central Mobile Standard	Subscription	per User	Maximum upload size: 25 MB for documents, 300 MB for apps

Intercept X for Mobile	Subscription	per User	N/A
Central Device Encryption	Subscription	per User	N/A
Central Email Advanced	Subscription	per User	N/A
Central Portal Encryption	Subscription	per User	Only available as an add-on for Central Email Advanced.
Zero Trust Network Access	Subscription	per User	Two deployment modes available: on premise and Sophos Cloud gateway. Following usage limitations apply to Sophos Cloud gateway mode: • average data transfer of 15GB per month per User.
Network Detection and Response	Subscription	per User and per Server	N/A
Central Phish Threat	Subscription	per User	Each user who is sent mail from Phish Threat is considered to benefit from the product and requires a User license.
Sophos Firewall purchased on hardware appliance			
Network Protection	Subscription	per hardware appliance	
Web Protection	Subscription	per hardware appliance	
Email Protection	Subscription	per hardware appliance	
Webserver Protection	Subscription	per hardware appliance	
Zero-Day Protection (for Sophos Firewall)	Subscription	per hardware appliance	
Xstream Protection	Subscription	per hardware appliance	Only applicable to Sophos Firewall The applicable use limitation(s) for DNS queries are provided below.

Firewall Model	Daily Query Limit
XGS88(w), XGS87(w), XG86(w), Virtual Firewall - 1C4 license	310,000
XGS108(w), XGS107(w), XG106(w), XG105(w), SG105(w)	390,000
XGS118(w),XGS116(w), XG115(w), SW115(w), Virtual Firewall - 2C4 license	480,000
XGS128(w),XGS126(w), XG125(w), SG125(w), Virtual Firewall - 4C6 license	600,000
XGS138,XGS136(w), XG135(w), SG135(w)	830,000
XGS2100, XG210, SG210	1,500,000
XGS2300, XG230, SG230, Virtual Firewall - 6C8 license	1,900,000
XGS3100, XG310, SG310	3,000,000
XGS3300, XG330, SG330, Virtual Firewall - 8C16 license	4,800,000
XGS4300, XG430, SG430	7,400,000
XGS4500, XG450, SG450	12,000,000
XGS5500, XG550,SG550, Virtual Firewall - Unlimited license	18,000,000
XGS6500, XG650, SG650	32,000,000

			XGS7500, XG750 53,000,000 XGS8500 120,000,000 DNS is not included in any consumption-based licensing.
Standard Protection	Subscription	per hardware appliance	Only applicable to Sophos Firewall
Central Orchestration	Subscription	per hardware appliance	Only applicable to Sophos Firewall
FullGuard	Subscription	per hardware appliance	Only applicable to UTM
Basic Guard	Subscription	per hardware appliance	Only applicable to UTM
Wireless Protection	Subscription	per UTM appliance	Only applicable to UTM
Sandstorm (for UTM)	Subscription	per hardware appliance	Only applicable to UTM
UTM Virtual Software			
FullGuard	Subscription	per User	When a User communicates with or through the gateway (including without limitation DNS and DHCP queries to the gateway and communications both to the Internet and a different LAN segment), their IP address is added to list of licensed devices in the gateway's local database. If several Users communicate through a single device then every User is counted as a separate User. If an IP address has not been used in the last seven (7) days, it is removed from the database.
Network Protection	Subscription	per User	
Web Protection	Subscription	per User	
Email Protection	Subscription	per User	
Wireless Protection	Subscription	per User	
Sandstorm	Subscription	per User	
Webserver Protection	Subscription	per User	
Sophos Firewall Virtual Software			
Base License	Perpetual	per virtual Computer	Selection of licenses by number of CPU cores and amount of memory is available
FullGuard	Subscription	per virtual Computer	
EnterpriseGuard	Subscription	per virtual Computer	
Network Protection	Subscription	per virtual Computer	
Web Protection	Subscription	per virtual Computer	
Email Protection	Subscription	per virtual Computer	
Webserver Protection	Subscription	per virtual Computer	
Xstream Protection	Subscription	per virtual Computer	The applicable use limitation(s) for DNS queries are provided below. Firewall model — Daily Query Limit XGS87(w), XG86(w), Virtual Firewall - 1C4 license — 310,000 XGS107(w), XG106(w), XG105(w), SG105(w) — 390,000 XGS116(w), XG115(w), SW115(w), Virtual Firewall - 2C4 license — 480,000 XGS126(w), XG125(w), SG125(w), Virtual Firewall - 4C6 license — 600,000 XGS136(w), XG135(w), SG135(w) — 830,000 XGS2100, XG210, SG210 — 1,500,000 XGS2300, XG230, SG230, Virtual Firewall - 6C8 license — 1,900,000 XGS3100, XG310, SG310 — 3,000,000 XGS3300, XG330, SG330, Virtual Firwall - 8C16 license — 4,800,000 XGS4300, XG430, SG430 — 7,400,000 XGS4500, XG450, SG450 — 12,000,000

			XGS5500, XG550, SG550, Virtual Firewall - Unlimited license: 18,000,000 XGS6500, XG650, SG650: 32,000,000 XGS7500, XG750: 53,000,000 XGS8500: 120,000,000 DNS is not included in any consumption-based licensing.
Standard Protection	Subscription	per virtual Computer	
Central Orchestration	Subscription	per virtual Computer	
Zero-Day Protection	Subscription	per virtual Computer	
Sophos Central Firewall Reporting			
Central Firewall Reporting Advanced	Subscription	GB storage capacity per Hardware appliance or per virtual Computer	A subscription includes a maximum number reports generated per Hardware appliance or per virtual Computer as follows: Report time range — Reports generated per month Last 24 hours — 2000 Last 7 days — 1000 Last 30 days — 200 Last 90 days — 80 90 days-1 year — 20
Other UTM Products			
UTM Endpoint Protection	Subscription	per User	Sold in license packs

Managed Services	Licensing Model	Applicable Unit(s)	Notes and Exceptions
Managed Detection and Response Essentials	Subscription	per User	One subscription includes 1 license to Central Intercept X Advanced with XDR.
Managed Detection and Response Complete	Subscription	per User	One subscription includes 1 license to Central Intercept X Advanced with XDR.
Managed Detection and Response Essentials Server	Subscription	per Server	One subscription includes 1 license to Central Intercept X Advanced for Server with XDR.
Managed Detection and Response Complete Server	Subscription	per Server	One subscription includes 1 license to Central Intercept X Advanced for Server with XDR.
Managed Risk	Subscription	per User and per Server	Available to Managed Detection and Response customers. The following limitations apply per customer: • 25 domains for asset monitoring • 1,000 IPs for vulnerability scanning.
Rapid Response	Subscription	per User and per Server	One subscription includes 1 license to Central Intercept X Advanced with XDR endpoint or server.
Compromise Assessment	Subscription	per Computer	One subscription includes a 7 day subscription to analysis of bands of Computers (5, 10, or 20 Computers).
Incident Response Retainer	Subscription	N/A	Entitlement includes a maximum number of device count applicable to customer's purchase.

Integration Pack Add-Ons and Data Retention	Licensing Model	Applicable Unit(s)	Notes and Exceptions
Network Detection and Response	Subscription	per User and per Server	Available to customers with Managed Detection and Response and Central Intercept X Advanced with XDR licenses (User and Server).

Public Cloud Integration Pack	Subscription	per User and per Server	
Email Integration Pack	Subscription	per User and per Server	
Firewall Integration Pack	Subscription	per User and per Server	
Network Integration Pack	Subscription	per User and per Server	
Back-up and Recovery Integration Pack	Subscription	per User and per Server	
Central Data Storage 1-year Pack	Subscription	per User and per Server	Available to customers with Central Intercept X Advanced with XDR license (User and Server). Only data sent to Sophos Data Lake from Sophos XDR-enabled products and from Integration Pack(s) are in scope. Central alert, report, threat graph, and audit data are not in scope. Licensed based on combined number of Users and Servers.

Sophos Factory	Licensing Model	Applicable Unit	Notes and Exceptions
Sophos Factory Pro	Subscription	per credit	Credits reset monthly.
Sophos Factory Enterprise	Subscription	per credit	Credits reset monthly.

Updated: 29 January 2025

Exhibit B

Sophos Hardware Terms

These Sophos Hardware Terms ("Hardware Terms") supplement, and are subject to, and form a part of Sophos End User Terms of Use attached hereto (the "Agreement"). Those terms of the Agreement that are applicable to Products generally shall be read to apply to Hardware, except as expressly varied or added to by these Hardware Terms. All capitalized terms used below shall have the meanings given to them in the Agreement. In the event of a conflict between the Agreement and these Hardware Terms, these Hardware Terms shall take precedence with respect to Hardware only.

1. USE RIGHTS AND RESTRICTIONS

(a) Hardware is to be used only with the Software that is pre-installed or made available for download to such Hardware. Subject to Customer's compliance with these Hardware Terms, Customer may use the Hardware to exercise its rights to the Software, as provided in the Entitlement. Customer may use the Hardware only with the Software and only for Customer's internal information security operations, unless otherwise agreed by the parties in writing.

(b) Customer may not disassemble the Hardware including without limitation, removing any labels, covering plates that bar access to the Hardware ports and/or accessing internal components of the Hardware, except as may be agreed by the parties in writing, or as may be directed by Sophos technical support personnel.

2. EVALUATION

(a) If the Hardware is provided to Customer for evaluation ("Loaned Hardware"), the evaluation term shall commence upon Sophos's or Partner's shipment of the Hardware, and shall continue for not more than sixty (60) days unless otherwise agreed by Sophos. The following additional terms apply to all Loaned Hardware:

(i) Sophos retains title to and all ownership rights in the Loaned Hardware,

(ii) Customer may only use the Loaned Hardware in non-production environments,

(iii) Customer must safeguard and protect all Loaned Hardware from possible damage until back in Sophos' possession,

(iv) Customer will not provide the Loaned Hardware to any third party,

(v) Customer will not allow any lien to be imposed upon the Loaned Hardware,

(vi) If there is any damage to the Loaned Hardware beyond normal wear or if the Loaned Hardware is lost or stolen, Customer will be liable for the full costs of repair or replacement, and

(vii) Upon expiration of the evaluation period, Customer must return the Hardware to the return location, and in the timeframe, indicated by Sophos, securely and properly packaged, with carriage (and insurance at Customer's option) prepaid. Customer is solely responsible for removing any and all of Customer's data from the Loaned Hardware prior to return. If Customer fails to return the Loaned Hardware as required Sophos or Partner may invoice, and Customer will pay the list price of the Loaned Hardware.

3. DELIVERY AND RISK OF LOSS.

3.1 Delivery. Hardware will be delivered in accordance with the then-current Sophos shipping terms. Sophos reserves the right to charge the costs of expedited carriage (e.g., overnight shipping services) upon Customer's prior written approval to Customer.

3.2 Risk of Loss. Risk of loss passes to Customer upon shipment of the Hardware to Customer. Insurance, if any, covering the Hardware shall be Customer's sole responsibility.

4. WARRANTY The warranty applicable to the Hardware is attached hereto as **Exhibit B-1** for reference.

5. REGULATORY COMPLIANCE

Customer is solely responsible for, and Sophos shall have no liability for, complying with governmental regulations relating to waste, health and safety, that are applicable to Customer's use, transport and/or disposal of the Hardware, including without limitation, those that relate to the EC Directive on Waste Electrical and Electronic Equipment (2002/96/EC) ("WEEE") and The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations (2002/95/EC) ("RoHS") (as amended) and similar local laws and regulations.

6. HARDWARE AVAILABILITY

6.1 Sophos may vary, update or discontinue the Hardware, or specific versions, features, support, maintenance, from time to time for reasons including but not limited to changes in demand or technology. Sophos will use commercially reasonable efforts to provide advance notice of any planned Hardware discontinuation (whether alone or as part of a Product) by publishing the date(s) of each planned discontinuation at https://www.sophos.com/en-us/support ("Retirement Calendar"). Customer acknowledges and agrees that it is Customer's sole responsibility to review the applicable Retirement Calendar.

6.2 Unless otherwise required by applicable law, Sophos will not provide a refund of fees paid for Hardware that is subject to a modification as described in this Section. Any refund that may be due under applicable law will, unless prohibited by applicable law, be calculated on a three (3) year straight line depreciation basis.

7. TRANSFER OF TITLE

Sophos retains title to the Hardware until such time as Customer pays the associated fee to Sophos or a Partner, as applicable. Unless and until title to the Hardware has transferred to Customer in accordance with this Section, Customer agrees to keep the Hardware free and clear of all claims, liens, and encumbrances. Customer acknowledges that it owns only the Hardware on which the Software is installed and does not acquire any rights to the Software by virtue of its ownership of the Hardware.

EXHIBIT B-1

Hardware Warranty Policy

Hardware Warranty Terms

These Hardware Warranty Terms supplement, are subject to and form part of the Sophos End User Terms of Use (the "Agreement") which is available at https://www.sophos.com/en-us/legal. All capitalized terms used below shall have same meaning as in the Agreement.

1. BASE WARRANTY. Sophos warrants that during the Base Warranty Period, the Hardware shall be free of defects in materials and workmanship and will perform substantially in accordance with the Documentation, when used in accordance with the Documentation.

2. BASE WARRANTY PERIOD. The base warranty period for the Hardware will run for 12 (twelve) months from the date Sophos processed the order from its channel partner (the "Base Warranty Period").

3. EXTENDED WARRANTY. Provided that Customer is the original purchaser (as evidenced by Sophos sales records, and except where otherwise required by law), Sophos warrants that during the Extended Warranty Period, the Hardware listed in Section 4 below, shall be free of defects in materials and workmanship and will perform substantially in accordance with the Documentation, when used in accordance with the Documentation.

4. EXTENDED WARRANTY PERIOD. The extended warranty period for the Hardware listed below will run from the date Sophos processed the order from its channel partner until expiry of the periods stated below (the "Extended Warranty Period"):

Hardware	Extended Warranty Period
• SD-RED • APX series	Five (5) years, but in no event beyond the End-of-Life Date
• Sophos Switch • AP6 series	Limited Lifetime Warranty For purposes of this warranty, the "Lifetime" of the Hardware ends on the End-of-Life Date.

"End-of-Life Date" means the respective end of life date, as updated by Sophos from time to time, and published at: https://support.sophos.com/support/s/article/KB-000035279?language=en_US

5. SOPHOS' OBLIGATION. If the eligible Customer notifies Sophos in writing of a breach of either of the above warranties during the relevant Warranty Period, Sophos' entire liability and Customer's sole remedy shall be (at Sophos' option and subject to these Hardware Warranty Terms): (i) to correct, repair or replace the Hardware and/or Documentation as applicable within a reasonable time, or (ii) provide, or authorize the appropriate Partner to provide, a refund of the Fee paid for such Hardware. Any refund authorized will be paid only following the return of the Hardware to the address provided by Sophos, accompanied by proof of purchase, and will be calculated on a three (3) year straight line depreciation basis. Any items provided as replacement under these Hardware Warranty Terms will be warranted only for the remainder of the respective original Warranty Period.

6. STANDARD HARDWARE REPLACEMENT

A. Upon perceived failure of the Hardware covered by the foregoing warranties; Customer is required to contact Sophos for a Return Merchandise Authorization ("RMA") number. Sophos will issue the requested RMA after Sophos determines that the Hardware is eligible for replacement.

B. Customer will return the defective Hardware or component part(s) of the Hardware to the return location designated by Sophos. It must be securely and properly packaged with carriage (and insurance at Customer's option) prepaid by Customer and the RMA number prominently displayed on the exterior of the packaging.

C. Upon receipt of the defective Hardware by Sophos, Sophos will (at its cost) ship replacement Hardware to Customer. Notwithstanding the foregoing, replacement Hardware may, at Sophos' sole discretion, be shipped before receipt by Sophos of the Hardware being returned.

D. If Sophos receives an automated failure notice from the Hardware, Sophos may issue an RMA to Customer and ship replacement Hardware without the need for Customer to contact Sophos. In such case, these Hardware Warranty Terms shall apply just as if Customer had placed a call for warranty coverage.

7. ADVANCE HARDWARE REPLACEMENT

A. For certain Hardware, Customer may be able to purchase a support contract that extends and/ or enhances the Hardware replacement cover. More information can be found at https://www.sophos.com/en-us/support/technical-support.

B. Any extension and/or enhancement under sub Section A above can in no event extend beyond the End-of-Life Date ("Supported Period").

C. Where a support contract for XG and XGS has been purchased more than thirty (30) days after expiry of (i) any applicable Warranty Period or (ii) the previous support contract, Customer will not be entitled to receive replacement Hardware during the first three (3) months of such support contract ("Waiting Period"), unless reinstatement is purchased at an additional fee to waive the Waiting Period.

D. If the Hardware is covered by a support contract which includes advance hardware replacement and the respective Hardware fails during the Supported Period, Customer is required to contact Sophos for an RMA.

E. Provided the request has not been raised during the Waiting Period, upon approval of the requested RMA, Sophos will ship the replacement Hardware to Customer before the defective Hardware is received by Sophos.

F. Upon Customer's receipt of the RMA, Customer must, within fifteen (15) calendar days, return the allegedly defective Hardware as directed by Sophos. Customer will use any packaging supplied by Sophos. If no packaging is supplied, Customer will package the defective Hardware in a manner designed to avoid further damage to the Hardware. In either case, Customer will ship the Hardware to Sophos, at Sophos's expense, via the carrier indicated by Sophos.

8. REPLACEMENT. Any replacement Hardware shipped under these Hardware Warranty Terms may, at Sophos' sole discretion, (i) be new or refurbished, (ii) be the same or a higher revision model, or (iii) Sophos may repair and return the same Hardware to Customer. The replacement Hardware might not be able to support the same Software (or the same release) used on the defective Hardware.

9. TITLE AND RISK. Title to the Hardware giving rise to a warranty/ support claim under these Hardware Warranty Terms shall pass to Sophos upon receipt by Customer of the replacement Hardware, or on receipt by Sophos of the defective Hardware at the return location indicated by Sophos, whichever is the sooner. Title to replacement Hardware provided to Customer under these Hardware Warranty Terms shall pass to Customer upon shipping by or on behalf of Sophos, or receipt of the defective Hardware by Sophos, whichever is the later. Risk of loss in relation to the replacement Hardware provided to Customer hereunder passes to Customer upon shipment of such Hardware by or on behalf of Sophos. Customer shall be responsible for obtaining and paying for any insurance desired by Customer.

10. NO FAULT FOUND. Should the Hardware returned by Customer: (i) be deemed by Sophos not to be defective or 'no fault found', or (ii) be missing any Hardware or components, Sophos will invoice Customer or direct the applicable reseller or distributor to invoice Customer, and Customer will pay the cost of any replacement Hardware that had been sent to Customer.

11. FAILURE TO RETURN HARDWARE. Where Sophos ships replacement Hardware before receipt of the defective Hardware and Customer fails to return the defective Hardware as requested within thirty (30) days of receiving the replacement Hardware, Sophos may at its sole discretion, and without further notice to Customer, invoice

- or direct the applicable reseller or distributor to invoice, Customer for the replacement Hardware and Customer will pay such invoice within thirty (30) days of the date of such invoice. Once payment is received by Sophos, title to the replacement Hardware shall pass to Customer.

12. DISCLAIMER. IN ADDITION TO THE WARRANTY DISCLAIMERS IN SECTION 7.2 OF THE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW SOPHOS DISCLAIMS ANY RESPONSIBILITY FOR MAINTAINING OR PROTECTING ANY CONFIGURATION SETTINGS OR DATA FOUND ON THE RETURNED HARDWARE OR COMPONENT PART THEREOF. CUSTOMER IS SOLELY RESPONSIBLE FOR REMOVING ANY AND ALL OF CUSTOMER'S DATA FROM THE DEFECTIVE HARDWARE BEFORE SHIPPING THE HARDWARE.

13. EXCLUSIONS

A. This Hardware replacement offer covers repair or replacement of the Hardware should it fail due to a manufacturing defect during the Warranty and/ or Supported Period. It does not apply to Software, configuration or configuration assistance, or any other Product, Service, or support. Sophos will replace Hardware with a like model or newer equivalent if the exact Hardware purchased is not available. Sophos does not guarantee backward compatibility of the replacement Hardware.

B. This Hardware replacement offer does not apply to:
(a) repair or replacement caused or necessitated by: (i) accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; fluctuations in electrical power beyond those set out in the specifications; failure of air conditioning or humidity control; improper maintenance, or any other neglect, misuse, abuse or mishandling; (ii) force majeure, including, without limitation, natural disasters such as fire, flood, wind, earthquake, lightning or similar disaster; (iii) governmental actions or inactions; (iv) strikes or work stoppages; (v) Customer's failure to follow applicable use or operations instructions or manuals; (vi) Customer's failure to implement, or to allow Sophos or its agents to implement, any corrections or modifications to the Hardware made available to Customer by Sophos; or (vii) such other events outside Sophos' reasonable control; and/or
(b) repair or replacement that would be contrary to Sanctions and Export Control Laws.

C. ALL HARDWARE WARRANTIES ARE NULL AND VOID IF ANY WARRANTY STICKERS ARE TAMPERED WITH OR ARE MISSING, OR IF THE HARDWARE WAS REPAIRED OR ALTERED BY PERSONNEL OTHER THAN THOSE AUTHORISED BY SOPHOS.

14. CHANGES. Non-material Changes to these Hardware Warranty Terms shall be effective thirty (30) days from the date Customer is advised of changes. Such notice may include posting of the revised Hardware Warranty Policy to this website.

Revision Date: 17 August 2023

EXHIBIT C

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") forms part of the Main Agreement and is effective between the Supplier and the Customer ***if***: (1) the Addendum is expressly incorporated by reference into the Main Agreement (as defined in clause 2) between **Sophos Limited**, a company registered in England and Wales number 2096520, with its registered office at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, UK ("Supplier") and the end customer ("Customer"), and (2) the Addendum is consistent with the Federal laws of the United States.

Capitalized terms used in this Addendum are defined as set forth in clause 2 below. Upon request we may be able to provide a copy of this Addendum in another language. In the event of a conflict, the English version of the Addendum shall control.

1. PREAMBLE

1.1. The parties have entered into the Main Agreement regarding the provision by the Supplier to the Customer of certain products and/or services (collectively, "Products").

1.2. If the Main Agreement is an MSP agreement in similar form to the MSP agreement located at https://www.sophos.com/en-us/legal/sophos-msp-partner-terms-and-conditions ("MSP Agreement"), the Customer is a managed service provider ("MSP"). If the Main Agreement is an OEM agreement under which the Customer is authorised to distribute, sublicense, or make available to third parties Supplier Products in combination with the Customer's products as part of a bundled unit ("OEM Agreement"), the Customer is an original equipment manufacturer ("OEM"). Otherwise, the Customer is an end user ("End User").

1.3. The provision of the Products may include the collection, use, and other processing of Controller Personal Data by the Supplier on behalf of Customer. This Addendum sets forth the obligations of the parties with respect to such Processing and supplements the terms and conditions of the Main Agreement.

1.4. Notwithstanding any other term of the Agreement or this Addendum, the parties agree that the Controller Personal Data shall not include contact information, payment or billing information, or other Personal Data about business contacts and Customer administrators, including name, email address and contact information, which Supplier collects and Processes on its own behalf in order to manage its customer relationships, communicate with current, former and prospective customers and business partners, and otherwise administer its business relationships ("CRM Data").

1.4.1. Supplier is a Controller for CRM Data and will Process CRM data in accordance with its obligations under Applicable Data Protection Law and the Supplier Group Privacy Notice.

1.4.2. Except with respect to Section 1.4.1, the obligations of Supplier pursuant to this Addendum shall not apply to CRM Data.

1.5. The Main Agreement, this Addendum and the documents expressly referenced in the Main Agreement and this Addendum shall constitute the entire agreement between the parties in relation to personal data collected, processed and used by the Supplier on behalf of the Customer in connection with the Main Agreement, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

2. DEFINITIONS

2.1. In this Addendum, the following terms shall have the following meanings:

“Applicable Data Protection Laws” means, to the extent applicable: (a) EU Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR"); (b) the e-Privacy Directive (EU Directive 2002/58/EC); (c) the CCPA; and (d) any and all applicable national data protection legislation, including legislation made under or pursuant to (a) or (b); in each case as may be amended or superseded from time to time.

“Beneficiary” has the meaning given to it in the MSP Agreement.

“CCPA” means the California Consumer Privacy Act as amended by the California Privacy Rights Act of 2020), codified at Cal. Civ. Code §§ 1798.100 - 1798.199.100 and the California Consumer Privacy Act Regulations issued thereto, Cal. Code Regs. tit. 11, div. 6, ch. 1, each as amended;

“Clauses” shall have the meaning ascribed to it in the SCCs.

“Controller” means either: (a) the Customer, if the Customer is an End User; (b) the Beneficiary, if the Customer is an MSP; or (c) the End Customer, if the Customer is an OEM.

“Controller Personal Data” means the Personal Data which Supplier Processes on behalf of Controller pursuant to the Services.

“Controller to Processor Clauses” means the Module Two Clauses to the SCCs.“CRM Data” means contact information, payment or billing information, or other Personal Data about business contacts and Customer administrators, including name, email address and contact information, which Supplier collects and Processes on its own behalf in order to manage its customer relationships, communicate with current, former and prospective customers and business partners, and otherwise administer its business relationships.

“Data Subject” means the individual to whom the Sophos Personal Data relates.

“Data Subject Requests” means any requests from Data Subjects exercising rights pursuant to Applicable Data Protection Laws including their rights of access, deletion and correction.

“EEA” means the European Economic Area, including (a) the Member States of the European Economic Area (“EEA”), and (b) the United Kingdom.

“End Customer” has the meaning given to it in the OEM Agreement.

"Europe" (and "European") means (a) the Member States of the European Economic Area (“EEA”), and (b) the United Kingdom.

“Hosted Products” mean the Products listed in Exhibit 3.

“ICO” means The Information Commissioner’s Office established in the United Kingdom

“Main Agreement” means, collectively, the written agreement(s), including and exhibits, addenda and amendments thereto, pursuant to which Supplier provides certain Services to Customer.

“Personal Data” means any information that identifies, could be used to identify or is otherwise linked or reasonably linkable with a particular individual or household, as well as any information defined as “personal data,” “personal information” or equivalent term under applicable Data Protection Laws and Regulations.

“Personal Data Breach” means a breach of security (other than those caused by the Customer or its users) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Personal Data processed by the Supplier under this Addendum.

“Processor” means a person or entity that Processes Personal Data on behalf and under the instructions of the Controller, including any entity acting as a “service provider” pursuant to the CCPA.

“Restricted Transfer” means a transfer of Controller Personal Data by Customer to Supplier, where such transfer would be prohibited by Applicable Data Protection Laws in the absence of the applicable Standard Contractual Clauses and where applicable the UK Addendum.

"Sensitive Data" means "special categories of personal data," "sensitive personal data," "sensitive data," and equivalent term as defined under Applicable Data Protection Laws.

"Services" means any and all products provided and/or services performed by Supplier pursuant to the Main Agreement.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by the European Commission implementing decision (EU) 2021/914 of 4 June 2021.

"Subprocessor" means any person or entity (excluding any employee of Supplier) or entity appointed by or on behalf of Supplier that processes Controller Personal Data.

"Supervisory Authority" means the competent regulatory authority with regard to applicable Data Protection Laws and Regulations, including where applicable a supervisory authority as defined under the GDPR.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the ICO, as amended or replaced from time to time by a competent Supervisory Authority under the relevant data protection laws of the UK

2.2. In this Addendum, the lower case terms "controller", "processor", "data subject", "personal data" and "processing" (and derivatives thereof) shall have the meanings given in Applicable Data Protection Law.

3. SCOPE

3.1. The subject matter and duration of the Supplier's processing of Controller Personal Data, including the nature and purpose of the processing, the types of Controller Personal Data to be processed, and the categories of data subjects, shall be as described in: (a) this Addendum; (b) the Main Agreement; (c) any instructions in Exhibit 1 (Data Processing Instructions); and (d) the Customer's instructions issued in accordance with clause 4 below.

3.2. The Customer is responsible for ensuring (a) that the Controller has a lawful basis for the processing of Controller Personal Data that will be carried out by the Supplier on Customer's behalf, and (b) that the Controller has obtained all necessary consents from data subjects that may be required for the processing of Controller Personal Data by the Customer and the Supplier (including but without limitation, in relation to Sensitive Data); and (c) that it is otherwise compliant with, and will ensure its instructions to the Supplier for the processing of Controller Personal Data comply in all respects with, Applicable Data Protection Laws.

3.3. The parties agree that Supplier is a Processor or Subprocessor for Controller Personal Data, and Customer is either (a) the Controller where Customer is an End User, or (b) a Processor ((for a third party controller) where Customer is an MSP or OEM.

4. CUSTOMER INSTRUCTIONS

4.1. Customer instructs Supplier to process the Controller Personal Data as reasonably necessary to provide and perform the Services and as otherwise set forth herein and in the Main Agreement. The Supplier shall process the Controller Personal Data in accordance with the Customer's documented processing instructions, as forth herein, except (a) where otherwise agreed in writing between the Supplier and the Customer; or (b) where required by law to which the Supplier is subject (in which event, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits the provision of such information).

4.2. If the Supplier becomes aware that the Customer's processing instructions infringe Applicable Data Protection Laws (without imposing any obligation on the Supplier to actively monitor the Customer's compliance), it will promptly notify the Customer of same and suspend processing of the Controller Personal Data.

4.3. Without limiting the forgoing, to the extent the California Consumer Privacy Act ("**CCPA**") applies to the Controller Personal Data, Supplier further agrees that:

4.3.1. Supplier will not use, disclose or otherwise process Controller Personal Data except for the specific purpose of performing the Services, in accordance with the terms of this Addendum and the Main Agreement, and as otherwise required by applicable laws. Notwithstanding the foregoing:

a. Supplier may engage Subprocessors to process Controller Personal Data, subject to the terms of Section 7;

b. Supplier will not process Controller Personal Data outside of the direct business relationship between Customer and Supplier or for Supplier's own commercial purposes; notwithstanding the foregoing, the Parties agree that to the extent the CCPA applies, Supplier will only Process the Controller Personal Data for the specific business purposes set forth in the Main Agreement and this Addendum or for another purpose expressly authorized pursuant the CCPA regulations.

c. Supplier will not "share" or "sell" (as those terms are defined under the CCPA) any Controller Personal Data;

d. Supplier will (and will procure that each Subprocessor will) comply with its obligations pursuant to the CCPA and will provide the same level of privacy protection as is required by the CCPA; and

e. If Supplier believes it will be unable to comply with the terms of this Addendum or Applicable Data Protection Laws, Supplier will promptly notify Customer and grant Customer the right to take reasonable and appropriate steps to ensure that the Controller Personal Data is processed in a manner that is consistent with the Controller's obligations under the CCPA.

f. Supplier will not retain Controller Personal Data upon the expiration or termination of the Main Agreement, except as set forth in Section **Error! Reference source not found.**;

5. DUTIES OF THE SUPPLIER

5.1. All Supplier personnel who process the Controller Personal Data shall be adequately trained with respect to their data protection, security and confidentiality obligations, and shall be subject to written or statutory obligations to maintain confidentiality.

5.2. The Supplier will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and to protect the Controller Personal Data against a Personal Data Breach. Such measures will take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons so as to ensure a level of security that is appropriate to the risk. In particular, the measures taken by the Supplier shall include those described in Exhibit 2 of this Addendum. The Supplier may change or amend the technical and organisational measures described in Exhibit 2 without the prior written consent of the Customer provided that the Supplier maintains at least an equivalent level of protection. Upon request by the Customer, the Supplier will provide an updated description of the technical and organisational measures in the form as presented in Exhibit 2.

5.3. The Supplier shall follow the requirements specified in clause 7 below for engaging any Subprocessor to process Controller Personal Data.

5.4. The Supplier shall follow the requirements specified in clause 8 below for assisting the Customer to respond to enquiries from third parties, including any requests from data subjects to exercise their rights under Applicable Data Protection Laws.

5.5. Upon confirming the occurrence of any Personal Data Breach, the Supplier shall inform the Customer without undue delay and shall provide all such timely information and cooperation as the Customer may reasonably require in order for the Customer (and, if the Customer is an MSP or OEM, its Controller) to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. The Supplier shall further take measures and actions as are reasonably necessary to remedy or mitigate the effects of the Personal Data Breach and shall keep the Customer informed of developments in connection with the Personal Data Breach.

5.6. The Supplier shall provide the Customer (or, if the Customer is an MSP or OEM, its Controller) with reasonable and timely assistance as the Customer (or, as applicable, the Controller) may require in order to conduct a data protection impact assessment or other assessment required to be conducted by Applicable Data Protection Laws and, if necessary, consult with its relevant data protection authority. Such assistance shall be provided at the Customer's expense.

5.7. The Supplier shall, unless otherwise required by applicable law, delete the Controller's Controller Personal Data within a reasonable period of time following termination or expiry of this Addendum, unless prohibited by applicable law. Upon request, Supplier will confirm to Customer that such Controller Personal Data has been deleted in accordance with this Addendum. If Supplier is required by applicable laws to retain any Controller Personal Data, the Supplier shall takes steps to ensure the continued confidentiality and security of the Controller Personal Data for so long as it is maintained.

6. AUDIT RIGHTS OF THE CUSTOMER

6.1. The Customer acknowledges that the Supplier is regularly audited against SSAE 18 SOC 2 standards by independent third party auditors. Upon reasonable request, the Supplier shall supply a copy of its SOC 2 audit report to the Customer, which reports shall be subject to the confidentiality provisions of the Main Agreement as the Supplier's confidential information. The Supplier shall also respond to reasonable written audit questions submitted to it by the Customer, provided that the Customer shall not exercise this right more than once per year.

6.2. If in Customer's reasonable opinion, the materials provided under clause 6.1 are insufficient to demonstrate Supplier's compliance with this Addendum, Customer may request in writing and subject to clause 6.2 (a) - (d) herein, that Supplier make available to Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this Addendum (including the Standard Contractual Clauses to the extent applicable) and allow for and contribute to audits, including inspections, by Customer or Customer's independent, third-party auditor that is not a competitor of Supplier of the Processing activities that are covered by this Addendum.

a. Prior to requesting a review or audit pursuant to this clause 6.2, Customer will take into account the relevant Supplier third-party certifications and audits described under clause 6.1;

b. Customer will give Processor reasonable notice, at least 60 days in advance, of a request to conduct an audit or inspection under this clause 6.2, and will take (and ensure that each of its auditors takes) reasonable measures to avoid and prevent any damage or injury and minimize any disruption from such audit or inspection;

c. An audit or inspection will be conducted no more than once annually, except where required by a Supervisory Authority or Applicable Data Protection Laws; and

d. Customer shall bear the full costs of any such audit and shall reimburse Supplier for reasonable costs and expenses incurred by Supplier pursuant to such audits, including any time expended by the Supplier, its Affiliates or its Subprocessors for any such audit or inspection at Supplier's then-current professional services rates, which shall be made available to Customer upon request.

7. SUBPROCESSORS

7.1. The Customer consents to the use of Supplier's existing Subprocessors as at the date of this Addendum, which are listed at https://www.sophos.com/en-us/legal ("Subprocessor List"), as well as the Supplier Affiliates. The Customer expressly consents to Supplier's engagement of additional third party Subprocessors (each a "New Subprocessor") subject to the terms set forth in this clause 7. The Supplier will provide Customer with thirty (30) days' notice prior to the addition of any New Subprocessor, which notice may be given by posting details of such addition to the Subprocessor List.

7.2. If the Customer does not object in writing to the Supplier's appointment of a New Subprocessor (on reasonable grounds relating to the protection of Controller Personal Data) within 30 days of the Supplier adding that New Subprocessor to the Subprocessor List, the Customer agrees that it will be deemed to have consented to that New Subprocessor. If the Customer provides such a written objection to the Supplier, the

Supplier will notify the Customer in writing within 30 days that either: (a) the Supplier will not use the New Subprocessor to process the Controller Personal Data; or (b) the Supplier is unable or unwilling to do so. If the notification in paragraph (b) is given, the Customer may, within 30 days of such notification, elect to terminate this Addendum and the Main Agreement as to the affected processing upon written notice to the Supplier and Supplier shall for Customers located within the European Economic Area and UK only, authorize a pro rata refund or credit of any prepaid fees for the period remaining after the termination. However, if no such notice of termination is provided within that timeframe, the Customer will be deemed to have consented to the New Subprocessor. The Supplier will impose data protection terms on New Subprocessors that impose equivalent protections for the Controller Personal Data as provided for by this Addendum. The Supplier will remain fully liable for the performance of each Subprocessor's obligations.

8. INQUIRIES OF THIRD PARTIES

8.1. The Supplier shall notify the Customer of any privacy request, correspondence, enquiry or complaint it receives from a data subject, regulator or other third party in connection with the processing of the Controller Personal Data providing full details of the same but shall not directly respond to the data subject, except where otherwise required by law.

8.2. To the extent necessary, the Supplier will provide reasonable and timely assistance to the Customer (or, if the Customer is an MSP or OEM, the Controller), at the Customer's expense, to enable the Customer (or if the Customer is an MSP or OEM, the Controller) to respond to: (a) a request from a data subject to exercise its rights under Applicable Data Protection Law (including where applicable, its rights of access, correction, objection, erasure and data portability, as and (b) a request received from a regulator or other third party in connection with the processing of the Controller Personal Data..

9. INTERNATIONAL DATA TRANSFERS

9.1. Certain Products may enable the Customer to select where to host the Controller Personal Data for such Products, including in data centres that may be located outside of the jurisdiction in which the data originates. Those locations may include (a) the European Economic Area, (b) the United Kingdom, (c) the United States of America; or another location as specified in the Main Agreement ("Central Storage Location"). This selection takes place at the point of Product installation, account creation, or first use of the relevant Product. Once selected, the Central Storage Location cannot be varied at a later date.

9.2. The Customer herby acknowledges and expressly consents, regardless of the selected Central Storage Location (if relevant), to Restricted Transfers, subject to compliance with the obligations set out in this clause 9.

9.3. With respect to any Restricted Transfers:

9.3.1. The SCCs and the UK Addendum are expressly incorporated hereto and form a part of this Addendum;

9.3.2. Subject to Section 9.3.3 and Exhibit 4 hereto, Customer and Supplier hereby enter into and agree to: (i) the SCCs, which shall apply to the extent of a Restricted Transfer of Controller Personal Data to Supplier; and (ii) the UK Addendum, which shall apply to, and modify and supplement the SCCs with respect to any Restricted Transfer of Controller Personal Data that is subject to the Data Protection Laws and Regulations of the United Kingdom; and

9.3.3. Module 2 of the SCCs shall apply, subject to the terms of Exhibit 4 hereto.

9.4. The Appendix to the SCC's shall be completed as set out in Exhibit 4 below.

10. DURATION

10.1. This Addendum commences upon (a) execution by both parties of the Main Agreement or (b) the date on which the Main Agreement becomes effective, if later and continues until the earlier of: (i) the expiry of the Customer's entitlement to use and receive the Products, as noted in the Main Agreement or on any associated license entitlement; and (ii) the termination of the Main Agreement.

11. OTHER REGULATIONS

11.1. Modifications of and amendments to this Addendum require the written form. This also applies to changes and modifications to this clause 11.1.

11.2. In no event shall the Supplier's liability to the Customer in connection with any issue arising out of, or in connection with, this Addendum exceed the Supplier's limitations on liability set out in the Main Agreement. The Supplier's limitations on liability as set out in the Main Agreement shall apply in aggregate across both the Main Agreement and this Addendum, such that a single limitation on liability regime shall apply across both the Main Agreement and this Addendum.

11.3. This Addendum shall (excluding the SCCs) be governed by and construed in accordance with the laws of England and Wales, without regard to conflict of laws principles. To the extent permitted by applicable law, the courts of England shall have exclusive jurisdiction to determine any dispute or claim that may arise out of, under, or in connection with this Addendum.

11.4. To the extent of any conflict with the terms of this Data Processing Addendum and the terms of any SCC's entered into by the parties, the terms of the applicable SCC's (including any Annexes thereto), shall take precedence.

12. CHANGES IN LAW

12.1. If any amendment to this Addendum is required as a result of a change in Applicable Data Protection Laws, then either party may provide written notice to the other party of that change in law. The parties will discuss and negotiate in good faith any necessary variations to this Addendum to address such changes. The parties will not unreasonably withhold consent or approval to amend this Addendum pursuant to this Section 12 or otherwise.

12.2. In the event the Standard Contractual Clauses or the UK Addendum are replaced, updated or superseded with a new version ("New Clauses"), Customer agrees that Supplier may, upon prior written notice to Customer, update this Addendum as necessary to incorporate such New Clauses, as an amendment to or replacement of the prior Standard Contractual Clauses or UK Addendum.

Exhibit 1

DESCRIPTION OF PROCESSING

This Exhibit 1 describes the processing that the Supplier will perform on behalf of the Customer.

(a) Subject matter, nature and purpose of the processing operations
The Controller Personal Data will be subject to the following basic processing activities (please specify):

- Providing the Products purchased by the Customer under and pursuant to the Main Agreement
- Providing account management and customer technical support services

The Supplier provides Products that are designed to detect, prevent, and manage, or assist the Supplier to detect, prevent, and manage security threats within or against systems, networks, devices, files, and other data made available by the Customer. The content of any information held in these systems, networks, devices, files and other data is determined solely by the Customer and not by the Supplier.

(b) Duration of the processing operations:
The Controller Personal Data will be processed for the following duration (please specify):

The duration specified in the Main Agreement (or for the term of the Main Agreement, if not otherwise specified).

(c) Data subjects
The Controller Personal Data concern the following categories of data subjects (please specify):

- Personnel and end users of Customers
- Other Data Subjects whose Personal Data is processed on behalf of Customer related to the Sophos Products

(d) Types of personal data
The Controller Personal Data concern the following categories of data (please specify):

- Usernames and other identifiers
- Network and network activity information
- Other information that may be transmitted or processed in connection with the Sophos Products

(e) Special categories of data (if appropriate)
The Controller Personal Data concern the following special categories of data (please specify):

Unless otherwise specified, the Supplier's Products are not designed to process special categories of data.

Exhibit 2

TECHNICAL AND ORGANISATIONAL MEASURES

Certain of these measures may only be relevant or applicable to Hosted Products.

1. Physical Access Control.
   (a) Sophos has a physical access control policy;
   (b) All staff carry ID / access badges;
   (c) Entrances to facilities are protected by access badges or keys;
   (d) Facilities are divided into (i) public access areas (such as reception areas), (ii) general staff access areas, and (iii) restricted access areas which may only be accessed by those personnel with an express business need;
   (e) Access badges and keys control access to restricted areas within each facility according to an individual's authorised access levels;
   (f) Access levels for individuals are approved by senior staff members and are verified on a quarterly basis;
   (g) Reception and/or security staff are present at entrances to larger sites;
   (h) Facilities are protected by alarms;
   (i) Visitors are pre-registered and visitor logs are maintained.

2. System Access Control.
   (a) Sophos has a logical access control policy;
   (b) The network is protected by firewalls at each Internet connection;
   (c) The internal network is segmented by firewalls based on application sensitivity;
   (d) IDS and other threat detection and blocking controls run on all firewalls;
   (e) Filtering of network traffic is based on rules that apply the principle of "least access";
   (f) Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
   (g) Access to all systems and applications is controlled by a secure log-on procedure;
   (h) Individuals have unique user IDs and passwords for their own use;
   (i) Passwords are strength tested and changes are enforced to weak passwords;
   (j) Screens and sessions automatically lock after a period of inactivity;
   (k) Sophos malware protection products are installed as standard;
   (l) Regular vulnerability scans are conducted on IP addresses and systems;
   (m) Systems are patched on a regular cycle with a prioritisation system for fast-tracking urgent patches.

3. Data Access Control.
   (a) Sophos has a logical access control policy;
   (b) Access rights are only granted to authorised personnel to the extent and for the duration necessary in order to perform their job roles and are reviewed quarterly;
   (c) Access to all systems and applications is controlled by a secure log-on procedure;
   (d) Individuals have unique user IDs and passwords for their own use;
   (e) Passwords are strength tested and changes are enforced to weak passwords;
   (f) Screens and sessions automatically lock after a period of inactivity;
   (g) Laptops are encrypted using Sophos encryption products;
   (h) Senders are directed to consider file encryption prior to sending any external email.

4. Input Control.
   (a) Access to all systems and applications is controlled by a secure log-on procedure;
   (b) Individuals have unique user IDs and passwords for their own use;
   (c) The Sophos Central Products use transfer layer encryption to protect data in transit;
   (d) Communication between the client software and the backend Sophos system is performed over HTTPS to secure the data in transit, establishing trust communication via certificates and server validation.

5. Subcontractor Control.
   (a) Subcontractors with access to data undertake an IT security vetting procedure prior to onboarding and as required thereafter;

(b) Contracts contain an appropriate confidentiality and data protection obligations based on the subcontractor's duties.

6. Availability Control.
(a) Sophos protects its premises from fire, flood and other environmental hazards;
(b) Back-up generators are available to maintain power supplies in the event of power outages;
(c) Data centres and server rooms use climate controls and monitoring;
(d) The Sophos Central system is load balanced and has failover between three sites, each running two instances of the software, any one of which is capable of providing the full service.

7. Segregation Control.
(a) Sophos maintains and applies a quality control process for the deployment of new customer products;
(b) Testing and production environments are separate;
(c) New software, systems and developments are tested prior to release to the production environment.

8. Organisational Control.
(a) Sophos has a dedicated IT security team;
(b) The Risk and Compliance team manage internal risk reporting and controls, which include reporting on key risks to management;
(c) An incident response process identifies and remedies risks and vulnerabilities on a timely basis;
(d) Each new employee undertakes data protection and IT security training;
(e) The IT Security department conducts quarterly security awareness campaigns.

Exhibit 3

HOSTED PRODUCTS

(a) Sophos Central
(b) Sophos Cloud Optix
(c) Central Device Encryption
(d) Central Endpoint Protection
(e) Central Endpoint Intercept X
(f) Central Endpoint Intercept X Advanced
(g) Central Mobile Advanced
(h) Central Mobile Standard
(i) Central Phish Threat
(j) Central Intercept X Advanced for Server
(k) Central Server Protection
(l) Central Mobile Security
(m) Central Web Gateway Advanced
(n) Central Web Gateway Standard
(o) Central Email Standard
(p) Central Email Advanced
(q) Central Wireless Standard
(r) Any other Sophos product that is administered and operated via Sophos Central

Exhibit 4

ADDITIONAL TERMS FOR RESTRICTED TRANSFERS

This Exhibit includes additional terms applicable to Restricted Transfers by or on behalf of Customer to Supplier, pursuant to the Addendum, as well as the information necessary to complete the Appendices (Annexes I – III) to the applicable SCCs.

By agreeing to the Addendum, the Parties agree to and thereby execute the SCCs in all relevant parts, subject to Section **Error! Reference source not found.** of the Addendum and the terms of this Exhibit.

1. Capitalized terms used but not defined in this Exhibit or otherwise in the Addendum, shall have the meanings ascribed to them under the SCCs and the UK Addendum as applicable.

2. Module 2 of the SCCs shall apply, subject to the terms of this Exhibit and the Appendix to the SCCs shall be completed with reference to Attachment A hereto.

3. For the purposes of the SCCs (Module 2):

3.1. Clause 7: the optional docking clause shall not apply;

3.2. Clause 9(a): Option 2 (General Authorization) shall apply and the data importer shall notify the data exporter in writing at least 30 days in advance of any intended changes.

3.3. Clause 11: the optional language shall not apply.

3.4. For purposes of Clause 13(a), the competent supervisory authority shall apply as follows:

3.4.1. Where the data exporter is established in an EU Member State, the supervisory authority will be the competent supervisory authority for the jurisdiction in which the data exporter is established;

3.4.2. Where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom, the competent supervisory authority shall be the UK Information Commissioner's Office;

3.4.3. Where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland, the Swiss Federal Data Protection and Information Commissioner shall act as the competent supervisory authority; and

3.4.4. Where the data exporter is not established in an EU Member State, the United Kingdom or Switzerland, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2), the supervisory authority will be the competent supervisory authority for the jurisdiction in which the data exporter's representative is established, namely the Data Protection Commissioner of Ireland.

4. For purposes of Clause 17 and Clause 18(b), respectively, the SCC's shall be governed by the laws of the Republic of Ireland disputes will be resolved before the courts of Ireland, except that: (i) where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland, the SCC's shall be governed by the laws of, and disputes will be resolved before the courts of, Switzerland; and (ii) where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom, the SCC's shall be governed by the laws of, and disputes will be resolved before the courts of, the United Kingdom.

5. **Additional Terms for Switzerland**. Where the data exporter is established in Switzerland or the Restricted Transfer is subject to the Data Protection Laws and Regulations of Switzerland: (i) references in the SCCs to "European Union", "Union" or "member state" shall mean Switzerland; (ii) references to the GDPR shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced); and (iii) the SCCs also apply to the transfer of information relating to an identified or identifiable legal entity to the extent such information is protected as Personal Data under the applicable Data Protection Laws and Regulations of Switzerland.

6. **Additional Terms for the United Kingdom**. Where the data exporter is established in the United Kingdom or the Restricted Transfer is subject to the Data Protection Laws and Regulations of the United Kingdom:

6.1. The SCCs shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum; and

6.2. For the purposes of Part One, Tables 1 and Table 2 are completed with reference Attachments A and B (as applicable) of this Exhibit, Table 3 is completed with reference to the information in this Exhibit, and for purposes of Table 4 the data importer may end the UK Addendum as set out in Section 19 of the UK Addendum.

Attachment A to Exhibit 4

APPENDIX TO THE SCCS (MODULE 2): CONTROLLER-TO-PROCESSOR RESTRICTED TRANSFERS

ANNEX I

A. LIST OF PARTIES

1. Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name	As provided to Supplier under the Main Agreement
Address	As provided to Supplier under the Main Agreement
Other information needed to identify the Organisation	As provided to Supplier under the Main Agreement
Contact person's Name: Position: Contact details:	As provided to Supplier under the Main Agreement
Activities relevant to the data transferred under these SCCs	As set out in clause 3 to the Addendum above
Role	Controller

Data Exporter Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Addendum.

2. **Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*.]

Name	Sophos Limited (for and on behalf of its EU and Swiss subsidiaries)
Address	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Other information needed to identify the Organisation	Registration number 2096520
Contact person's Name: Position: Contact details:	Privacy Counsel dataprotection@sophos.com

Activities relevant to the data transferred under these SCCs	In accordance with the Agreement

Data Importer Signature and Date: The SCCs (Module 2), together with this Appendix and the Annexes herein, are executed as part of the Addendum.

B. DESCRIPTION OF TRANSFER

1.1. Categories of *data subjects whose personal data is transferred.*

As set forth in Exhibit 1, Part A.

1.2 Categories of *personal data transferred.*

As set forth in Exhibit 1, Part A.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature *of the processing*

Providing the Services procured by Sophos under and pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Supplier will process Controller Personal Data as necessary to perform the Services pursuant to the Agreement and as instructed by Sophos in its use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subject to Section 10 of the Addendum, Supplier will process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Supplier is authorised the to use the Sub-processors as notified by Supplier to Sophos at the time of execution of the Agreement or the Addendum.

C. COMPETENT SUPERVISORY AUTHORITY

As set out in Section 3.4 of Exhibit 4 to the Addendum.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As set forth in Exhibit 2 to the Addendum.

ANNEX III – LIST OF SUB-PROCESSORS

Not applicable (The parties have agreed to Option 2 (General Authorization) with respect to Clause 9 (a) of the SCCs).