

MSSP ADDENDUM FOR SAAS SOLUTIONS – GLOBAL PARTNER AGREEMENT

THIS ADDENDUM IS INCORPORATED BY REFERENCE INTO THE SECUREWORKS GLOBAL PARTNER AGREEMENT AVAILABLE AT <https://www.secureworks.com/terms-conditions/channel-partner-program-en> (INCLUDING AMENDMENTS, ADDENDUMS OR SUPPLEMENTS, THE “**AGREEMENT**”). BY ACCEPTING THIS MSSP ADDENDUM INCLUDING ALL APPLICABLE TERMS REFERENCED HEREIN AS BEING INCORPORATED INTO AND GOVERNED BY THE TERMS OF THIS DOCUMENT (“**MSSP ADDENDUM**” OR “**ADDENDUM**”), YOU REPRESENT AND WARRANT THAT YOU HAVE AUTHORITY TO BIND THE INDIVIDUAL OR ENTITY IDENTIFIED IN THE REGISTRATION PROCESS FOR THE PARTNER PROGRAM, AND YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS ADDENDUM. PLEASE ENSURE THAT YOU RETAIN A COPY OF THE AGREEMENT FOR YOUR RECORDS. WHEN YOU HAVE ACCEPTED THESE TERMS, YOU WILL BE REFERRED TO AS MSSP. THE EFFECTIVE DATE OF THIS ADDENDUM IS THE DATE YOU ACCEPT THIS MSSP ADDENDUM. UNLESS OTHERWISE SPECIFIED HEREIN, ALL CAPITALIZED TERMS NOT DEFINED HEREIN SHALL HAVE THE MEANINGS SET FORTH IN THE AGREEMENT. THIS MSSP ADDENDUM CONSTITUTES A SUPPLEMENT TO THE AGREEMENT FOR MSSPS. ALL TERMS OF THE AGREEMENT SHALL REMAIN IN FULL FORCE AND EFFECT EXCEPT TO THE EXTENT THIS MSSP ADDENDUM EXPRESSLY MODIFIES OR CONFLICTS WITH THE TERMS THEREOF, IN WHICH CASE THE TERMS IN THIS MSSP ADDENDUM SHALL TAKE PRECEDENCE.

1. ORDER PROCESS AND TERM; TERRITORY.

- 1.1 **Orders.** MSSP shall execute an Order with Secureworks or an authorized distributor for the SaaS Solution. Unless otherwise agreed to by Secureworks, an Order will set forth the name of each Customer, Customer’s address, email address, unique order identifier that is made available by Secureworks to Customer and an Order Term (as defined below).
- 1.2 **Term of Access to SaaS Solutions.** Access and use of the SaaS Solutions for each Customer shall commence upon execution of the Order and shall continue in effect until the earlier of (i) the termination or expiration of this Addendum, or (ii) the termination or expiration of the applicable Order (each, an “**Order Term**”).
- 1.3 **Territory.** Notwithstanding the provisions in the Agreement and for purposes of this MSSP Addendum only, the Territory (as defined in the Agreement) shall be worldwide, subject to the Orders being accepted by Secureworks.

2. ADDITIONAL LICENSES.

- 2.1 **Right to Use.** Secureworks will provide MSSP with access and use of the SaaS Solution, and any written directions and/or policies relating to the SaaS Solution (the “**SaaS Documentation**”) as necessary for MSSP to receive the SaaS Solution. Unless otherwise set forth herein, during the term of this Addendum, Customers will be considered customers of MSSP and not subject to the EULA Terms.
- 2.2 **Resale License.** Subject to the terms and conditions of this Addendum and the Agreement (including MSSP’s obligation to pay the fees), Secureworks grants to MSSP a non-exclusive, non-transferable, revocable right and license to: (i) sublicense the SaaS Solution to MSSP’s Customer solely as bundled with the MSSP Solution (as defined below) and (ii) access and use the SaaS Solutions solely as part of the MSSP Solution for use by and on behalf of its Customers. MSSP’s usage of the SaaS Solution is limited to the licensed volume stated on an Order (the “**Licensed Volume**”). As used in this Addendum, “**MSSP Solution**” means the managed services provided by MSSP to its Customers in the form of hardware, hosting, software integration, technology outsourcing, etc. of which each of the SaaS Solutions are one component of a broader product or service offering.
- 2.3 **Not-For-Resale License.** Subject to the terms and conditions of this Addendum and the Agreement (including MSSP’s obligation to pay the fees), Secureworks grants to MSSP a non-exclusive, non-transferable, revocable right and license to the SaaS Solution (i) to perform demonstrations and marketing to potential and current Customers, and (ii) for training and customer support for MSSP’s staff and Customers (the “**NFRS License**”). MSSP shall not use any such NFRS License in a production environment.
- 2.4 **Customer Owned License.** In the event that Customer has acquired the SaaS Solution directly from Secureworks or from a Secureworks designated third party reseller separate from the MSSP Solution, the license to use the SaaS Solution shall be held by Customer and Customer shall be subject to the EULA Terms. Upon request of Customer, MSSP shall have the right to access and use the SaaS Solutions solely as part of the MSSP Solution for use by and on behalf of its Customer(s); provided

that, MSSP has delivered to Secureworks an executed Authorization Form from Customer. Authorization Forms are located on the Partner Portal and once completed, should be sent to mssp@secureworks.com.

- 2.5 **Internal Use License.** Notwithstanding anything to the contrary set forth in the Agreement, MSSP may order the SaaS Solution for its own internal security end use in accordance with the terms and conditions set forth in this Addendum and, in this scenario, the Data Protection Addendum available at <https://www.secureworks.com/dpa/dpa-us> ("**Customer DPA**") shall apply in lieu of the DP Schedule.
- 2.6 **Termination of License.** Upon any termination or expiration of the Agreement, the license granted under this Addendum shall terminate in accordance with Section 9.4 of the Agreement, and MSSP shall certify in writing that all copies of the SaaS Solution have been destroyed.

3. RESTRICTIONS ON USE.

- 3.1 **General Restrictions.** Except as expressly permitted under this Addendum or otherwise approved in writing by Secureworks, the rights granted to MSSP are subject to the following restrictions and MSSP agrees not to: (i) integrate the software that provides the SaaS Solution with other software or services or display the SaaS Solution within another user interface or application in a manner which hides the actual URL or the Secureworks origin of the SaaS Solution; (ii) distribute, sublicense, lease, rent, loan, or otherwise transfer the SaaS Solution to any third party or permit any third party to benefit from the use or functionality of the SaaS Solution via timesharing, service bureau arrangements or otherwise; (iii) open, disassemble, or tamper with any hardware in any fashion; (iv) transfer possession of any hardware to any third party other than a Customer; (v) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the software that is embedded in the hardware or that provides the SaaS Solution; or work around any technical limitations in the SaaS Solution; (vi) publish (or otherwise make available) the SaaS Solution or SaaS Documentation or any programs or materials resulting from or relating to the SaaS Solution; (vii) use the SaaS Solution to upload, input, store or transmit infringing, libelous, or otherwise unlawful or tortious material (or to store or transmit material in violation of law or third-party privacy rights); (viii) perform or disclose any of the following security testing of the SaaS Solution or associated infrastructure: network discovery, port and service identification, vulnerability scanning, password cracking, remote access testing, or penetration testing; (ix) access or use the SaaS Solution for purposes of competitive analysis of the SaaS Solution, the development, provision, or use of a competing software service or product or any other purpose that is to Secureworks' detriment or commercial disadvantage; (x) use the SaaS Solution in a way intended to access or use the underlying infrastructure or to avoid incurring fees or exceed usage limitations; (xi) use or access the SaaS Solution in a manner not permitted by or otherwise inconsistent with this Addendum or Order; (xii) bypass or breach any security device or protection used by the SaaS Solution or access or use the SaaS Solution other than by a user through the use of his or her own then valid access credentials; or (xiii) charge any fee for the use or results of a trial subscription. MSSP must not remove, alter, or obscure in any way all proprietary rights notices (including copyright notices) of Secureworks or its suppliers on or within the copies of the SaaS Solutions. In all cases, MSSP will market the SaaS Solutions only as part of the applicable MSSP Solutions, and in no event will MSSP market the SaaS Solutions as a "free" component of a product or service offering sold by MSSP.
- 3.2 **Specific Restrictions.** MSSP shall not enter into an agreement regarding the MSSP Solution that would require Secureworks to provide the SaaS Solutions in a way not contemplated by this MSSP Addendum or that would obligate Secureworks to any additional legal or regulatory requirements not contemplated herein including, without limitation, laws or regulations requiring the localization of data, restrictions on data transfers, or that would require the provision of source code to any person.
- 3.3 **Monitoring of SaaS Solution.** MSSP will monitor its own use of the SaaS Solution and report any use in excess of the Data Cap (as defined in Section 4.5 below) or the Licensed Volume under an Order. Secureworks may monitor MSSP's use of the SaaS Solution under this Addendum at any time during an Order Term to verify compliance with the Data Cap, Licensed Volume, the Agreement, and this Addendum. If Secureworks determines that MSSP's use of the SaaS Solution exceeded the Data Cap or the Licensed Volume, MSSP shall pay to Secureworks all amounts due for such excess use. MSSP shall make all payments required under this Section 3.3 within thirty (30) days of the date of written notification of the audit results.

4. ADDITIONAL REQUIREMENTS, TRAINING, SERVICE LEVELS AND SUPPORT.

- 4.1 **Additional Requirements.** MSSP's eligibility to act as an MSSP is subject to additional obligations or conditions such as additional training, specialization requirements, and other conditions further described in the MSSP Documentation set forth on the Partner Portal (the "**MSSP Documentation**").

- 4.2 **Training and Support.** MSSP shall be the primary point of contact for all Customer support issues. Secureworks will provide training to MSSP's employees regarding the use of the SaaS Solutions and support services in accordance with the MSSP Documentation.
- 4.3 **Service Levels.** Secureworks will provide support and maintain SaaS Solution performance according to the service levels as follows (each a "**Service Level Commitment**"):

Taegis XDR: https://docs.ctpx.secureworks.com/legal/tdr_sla/
Taegis VDR: <https://support.delvsecurity.com/en/product-sla>

For clarity, all references in the Service Level Commitment documents to "Customer" shall mean "MSSP" for the purposes of this Addendum. The Service Level Commitment is subject to the exclusions in the links set forth above (the "Exclusions"). If MSSP provides a service credit to Customer(s) due to the failure of Secureworks to meet the then current Service Level Commitment, and none of the Exclusions apply, then MSSP will be entitled to a service credit from Secureworks, which will be calculated based on the fees paid to Secureworks corresponding to the Customer(s) to whom MSSP paid a service credit. The service credit remedy set forth in this section is MSSP's sole and exclusive remedy for the unavailability of the SaaS Solution(s). MSSP shall not be permitted to receive any service credits for unavailability of the SaaS Solution ordered pursuant to Section 2.5.

- 4.4 **Maintenance.** From time to time, Secureworks will perform scheduled maintenance of the systems related to the SaaS Solution. Secureworks shall use reasonable efforts to provide MSSP with at least twelve (12) hours' advance notice of any planned maintenance that affects the availability of the SaaS Solution.
- 4.5 **Taegis™ XDR Data Cap and Extended Retention.** MSSP's use of the SaaS Solution Taegis XDR shall be limited to the processing of not more than 4GB of MSSP Data processed per month multiplied by the Licensed Volume under each Order (the "**Data Cap**"). MSSP must purchase an upgraded volume for the Data Cap pursuant to an Order if MSSP's use exceeds the Data Cap. Secureworks' data retention policy for the SaaS Solution Taegis XDR can be found at https://docs.ctpx.secureworks.com/legal/tdr_data_retention/. Per this policy, MSSP may purchase an extend retention enhancement pursuant to an Order on a per Customer basis.

5. DATA AND SECURITY.

- 5.1 **Password Protection.** MSSP agrees to maintain the privacy of MSSP's and its employees' access credentials associated with the SaaS Solutions. MSSP has and will retain sole responsibility for the security and use of MSSP's and its employees' access credentials and all access to and use of the SaaS Solutions directly or indirectly by or through the employees' access credentials, with or without MSSP's knowledge or consent, including all results obtained from, and all conclusions, decisions, and actions based on, such access or use. MSSP agrees to (a) notify Secureworks as soon as possible of any unauthorized use of MSSP's password, MSSP's Internet account or any other breach of security; and (b) ensure that MSSP exits from MSSP's Internet account at the end of each session. Secureworks shall not be liable for any damages incurred by MSSP or any third party arising from MSSP's failure to comply with this Section 5.1.
- 5.2 **Suspension.** Secureworks may suspend, terminate, or otherwise deny MSSP's, any employee's, or any other person's access to or use of all or any part of the SaaS Solutions, without any obligation or liability, if: (a) Secureworks determines that it is required due to a judicial or other governmental demand or order, subpoena, or law enforcement request; or (b) Secureworks believes, in its good faith and reasonable discretion, that: (i) MSSP or any of its employees has failed to comply with any term of the Agreement or this Addendum, or accessed or used the SaaS Solutions in a manner that exceeds the rights granted pursuant to the Agreement or this Addendum, or for a purpose not authorized under the Agreement or this Addendum, or in any manner that does not comply with any instruction or requirement of the SaaS Documentation published by Secureworks; or (ii) MSSP or any of its employees is, has been, or is likely to be involved in any fraudulent, misleading, abusive, or unlawful activities relating to or in connection with any of the SaaS Solutions; or (c) MSSP fails to complete Partner training required under the Agreement and this Addendum. This Section does not limit any of Secureworks' other rights or remedies, whether at law, in equity, or under the Agreement or this Addendum.
- 5.3 **Security Procedures and DPA.** Secureworks shall maintain reasonable and appropriate safeguards designed to (a) reasonably protect MSSP Data (as defined below) in Secureworks' possession from unauthorized use, alteration, access or disclosure (a "**Security Breach**"); (b) detect and prevent against a Security Breach; and (c) ensure that Secureworks' employees and agents are trained to maintain the confidentiality and security of MSSP Data in Secureworks' possession. Secureworks shall promptly notify MSSP upon becoming aware of a confirmed Security Breach of MSSP Data or MSSP Confidential Information in Secureworks' possession or control. This Addendum also

incorporates the Data Protection Schedule attached hereto (“**DP Schedule**”), the Standard Contractual Clauses Schedule (“**SCC Schedule**”) and the UK and Swiss Amendments Schedule (“**UK/Swiss Amendments Schedule**”). MSSP acknowledges and agrees that researchers within the Secureworks Counter Threat Unit™ (CTU™), personnel within Secureworks’ CISO team, and Secureworks’ platform engineers may access Customer data within the SaaS Solution. No other Secureworks personnel may access Customer data within the SaaS Solution unless approved by a representative from MSSP on a case-by-case basis. Such approval may be evidenced via email from a representative of the MSSP service delivery team.

- 5.4 **Customer Data.** MSSP agrees that it will include in its agreement(s) with Customers and, in addition, also prominently display to Customers via any reasonably available means, a privacy notice that describes to Customers the information that is collected by MSSP and Secureworks and how such information is used, shared and otherwise processed in accordance with this Addendum and the Agreement. To the extent that MSSP transmits, stores, or processes Customer data outside of the SaaS Solutions, MSSP shall not: (i) modify the Customer data in a manner that adversely affects the integrity of that Customer data relative to the SaaS Solutions; or (ii) disclose Customer data to any third party without the consent of the Customer (which may be in the form of the agreement with the Customer).

6. PROPRIETARY RIGHTS.

- 6.1 **MSSP Proprietary Rights.** MSSP represents and warrants that it has the necessary rights, power and authority to transmit MSSP Data to Secureworks under this Addendum and that MSSP has and shall continue to fulfill all obligations as required to permit Secureworks to carry out the terms hereof, including with respect to all applicable laws, regulations and other constraints applicable to MSSP Data. As between MSSP and Secureworks, MSSP will own all right, title and interest in and to (i) any data provided by MSSP and/or its Customer(s) to Secureworks and/or any such data accessed or used by Secureworks or transmitted by MSSP and/or its Customer(s) to Secureworks or in connection with Secureworks’ provision of the SaaS Solution, including, but not limited to, any such data included in any written or printed summaries, analyses or reports generated in connection with the SaaS Solution (collectively, the “**MSSP Data**”), (ii) all intellectual property, including patents, copyrights, trademarks, trade secrets and other proprietary information (“**IP**”) of MSSP that may be made available to Secureworks in the course of providing SaaS Solution under this Addendum, and (iii) all confidential or proprietary information of MSSP or its Customer(s) including, but not limited to, MSSP Data, and other MSSP files, documentation and related materials, in each case under this clause (iii) obtained by Secureworks in connection with this Addendum. MSSP grants to Secureworks a limited, non-exclusive license to use the MSSP Data to perform the SaaS Solution. MSSP grants to Secureworks a limited, non-exclusive, perpetual, worldwide, irrevocable license to use and otherwise process Security Event Data (as defined below) during and after the term hereof to develop, enhance and/or improve its security services and the products and services it offers and provides to its customers, including MSSPs. “**Security Event Data**” means information collected during Secureworks’ provision of SaaS Solutions related to security events. This Addendum does not transfer or convey to Secureworks or any third party any right, title or interest in or to the MSSP Data or any associated IP rights except as set out in (and revocable in accordance with) this Addendum.
- 6.2 **Secureworks’ Proprietary Rights.** As between MSSP and Secureworks, Secureworks will own all right, title and interest in and to the SaaS Solution. This Addendum does not transfer or convey to MSSP or any third party, any right, title or interest in or to the SaaS Solution or any associated IP rights, but only a limited right of use as granted in and revocable in accordance with this Addendum. In addition, MSSP agrees that Secureworks is the owner of all right, title and interest in all IP in any work, including, but not limited to, all inventions, methods, processes, and computer programs including any source code or object code, (and any enhancements and modifications made thereto) contained within the SaaS Solution (collectively, the “**Background IP**”), developed by Secureworks in connection with the performance of the SaaS Solution hereunder and of general applicability across Secureworks’ customer base, and MSSP hereby assigns to Secureworks all right, title and interest in and to any copyrights that MSSP may have in and to such Background IP; provided, however, that such Background IP shall not include MSSP’s Confidential Information, MSSP Data, or other information belonging, referencing, identifying or pertaining to MSSP or MSSP’s Customer(s). During the term of the SaaS Solution, Secureworks grants to MSSP a limited, non-exclusive license to use such Background IP solely for MSSP to receive and use the SaaS Solution for MSSP’s Customer(s)’ internal security purposes only. Any license to the SaaS Solution expires or terminates upon the expiration or termination of this Addendum.
- 6.3 **Required Consents.** MSSP is responsible for, and will promptly obtain, maintain, and comply with, any required licenses, approvals, permits, or consents necessary to receive and use the SaaS Solution and to provide or permit Secureworks to access or process the MSSP Data. MSSP represents and warrants that it: (a) has the necessary rights, consents, approvals, licenses, power and authority to transmit MSSP Data to Secureworks and to permit Secureworks to provide the SaaS Solution, satisfy its obligations under this Addendum and process the MSSP Data in accordance with the DP Schedule;

and (b) has and shall continue to fulfill all obligations with respect to individuals as required to permit Secureworks to carry out the terms and satisfy its obligations under this Addendum, including with respect to all applicable laws, regulations and other constraints applicable to MSSP Data.

7. WARRANTIES AND LIABILITY.

- 7.1 **Warranties.** SECUREWORKS WARRANTS THAT: (I) DURING THE TERM OF EACH ORDER, THE SAAS SOLUTION SHALL CONFORM IN ALL MATERIAL RESPECTS TO THE SAAS DOCUMENTATION, AND (II) IN PROVIDING THE SAAS SOLUTION, SECUREWORKS WILL NOT KNOWINGLY INTRODUCE ANY VIRUS, DISABLING OR MALICIOUS SOFTWARE, CODE, OR COMPONENT THAT MAY LOCK, DISABLE, OR ERASE ANY MSSP DATA OR SOFTWARE. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 7.1, SECUREWORKS MAKES NO EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO THE SAAS SOLUTION, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR SUITABILITY. MSSP UNDERSTANDS THAT SECUREWORKS' SAAS SOLUTIONS DO NOT CONSTITUTE ANY GUARANTEE OR ASSURANCE THAT THE SECURITY OF MSSP'S CUSTOMER(S)' SYSTEMS, NETWORKS AND ASSETS CANNOT BE BREACHED OR ARE NOT AT RISK.
- 7.2 **Indemnification.** MSSP shall defend, indemnify and hold harmless Secureworks and its assignees, agents, officers and employees from any Claims related to (i) any violation of the use restrictions as to Secureworks' IP (including without limitation Background IP), and (ii) any allegation that the MSSP Data infringes any IP rights enforceable in the country(ies) where the MSSP Data is accessed, provided to or received by Secureworks or was improperly provided to Secureworks in violation of any person's rights, MSSP's or Customer(s)' privacy policies or applicable laws (or regulations promulgated thereunder).
- 7.3 **Compliance Disclaimer.** MSSP understands that, although Secureworks' SaaS Solution may assist MSSP in meeting certain compliance and regulatory use cases for its Customers, the Secureworks SaaS Solution is not designed for compliance and regulatory use. In addition, any written summaries or reports produced by Secureworks or generated by the SaaS Solution shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to MSSP legal or regulatory compliance.

8. MISCELLANEOUS.

- 8.1 **Feedback, Residual Knowledge, and General Information.** Secureworks shall own all right, title, and interest in and to any suggestions, enhancement requests, recommendations or other feedback provided by MSSP, including, without limitation, any IP in such suggestions, enhancement requests, recommendations, or feedback. Notwithstanding anything to the contrary contained in the Agreement or this Addendum, MSSP (a) acknowledges and agrees that Secureworks is free to use its general knowledge, skills and experience, and any ideas, concepts, know-how and techniques, related to or derived from the performance of the SaaS Solutions and (b) authorizes Secureworks to collect, use, disclose, create derivative works from, and modify in perpetuity information or data (including, but not limited to, general usage information) that is provided by MSSP in connection with the use or receipt of the SaaS Solutions (or generated, collected, or created in the course of Secureworks providing the SaaS Solutions) for the purposes of developing, improving, optimizing, and delivering SaaS Solutions and for Secureworks' own internal business purposes; provided, that any disclosure of such information or data shall not include Confidential Information of MSSP.
- 8.2 **Legal Proceedings.** If Secureworks is requested by MSSP, or required by government regulation, regulatory agency, subpoena, or other legal process to produce any reports, SaaS Documentation, other documentation or Secureworks personnel for testimony or interview with respect to the SaaS Solution, MSSP will: (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks for: (a) its employees' time spent as to such response at the hourly rate, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. MSSP will reimburse Secureworks' and its counsel's expenses and professional time incurred in responding to such a request. Nothing in this Section 8.2 shall apply to any legal actions or proceedings between MSSP and Secureworks as to the SaaS Solution.
- 8.3 **Governing law.** The law governing this MSSP Addendum and the DP Schedule shall be the same law governing the Agreement.
- 8.4 **Execution.** Acceptance of this MSSP Addendum after the date of publication hereof will be deemed to be execution of this Addendum.

DATA PROTECTION SCHEDULE

This Data Protection Schedule (“**DP Schedule**”) is incorporated into and forms part of the MSSP Addendum between MSSP and Secureworks. Capitalized terms not defined in this DP Schedule have the meaning set out in the MSSP Addendum – all other terms are defined below.

Except as otherwise expressly stated, this DP Schedule applies solely where Secureworks processes Personal Data (as defined below) as a processor in connection with the provision of SaaS Solutions under the MSSP Addendum. For the purpose of this DP Schedule (except where otherwise expressly stated) (i) Customer is the controller and (ii) MSSP and Secureworks are the processors, of Personal Data processed pursuant to the MSSP Addendum. Secureworks’ obligations regarding the processing of Personal Data are strictly limited to those set out in this DP Schedule and any additional obligations (including any additional security measures) agreed between a Customer and MSSP in a Customer Agreement shall not apply to Secureworks unless Secureworks has expressly stated otherwise in writing. In the event of a conflict between this DP Schedule, the MSSP Addendum and the Customer Agreement, this DP Schedule shall control with respect to its subject matter.

1. **Definitions:** References in this DP Schedule to “**controller**”, “**data subject**”, “**personal data**” (lower cased), “**processor**”, “**processing**” (and its derivatives) and “**supervisory authority**” shall have the meanings ascribed to them under the General Data Protection Regulation 2016/679 (the “**GDPR**”). References to “**business**”, “**consumer**”, “**sell**”, “**business purpose**” and “**commercial purpose**” shall have the meanings ascribed to them under the California Consumer Privacy Act of 2018 (the “**CCPA**”). In this DP Schedule:
 - 1.1 “**Customer Agreement**” means the applicable written agreement entered into by MSSP and a Customer regarding the MSSP Solution.
 - 1.2 “**Data Breach**” means an actual breach by Secureworks of the security obligations under this DP Schedule leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise processed.
 - 1.3 “**EU**” means the European Union consisting of the European member states from time to time.
 - 1.4 “**Personal Data**” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, which is processed by Secureworks, acting as a processor under the MSSP Addendum in anticipation of, in connection with or incidental to the performance of the SaaS Solutions under the MSSP Addendum. Personal Data includes, but is not limited to, the data elements listed in section 140(o)(1)(A)-(K) of the CCPA, if any such data element identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular individual or household.
 - 1.5 “**Privacy Laws**” means any data protection and/or privacy related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party to the MSSP Addendum is subject and which are applicable to the SaaS Solutions including, without limitation, the GDPR, the United Kingdom Data Protection Act 2018 (“**UK DPA**”), the United Kingdom GDPR (as defined in section 3 of the UK DPA, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018), and the CCPA.
 - 1.6 “**SCCs**” or “**Standard Contractual Clauses**” means the Standard Contractual Clauses (Module One: controller to controller and Module Three: processor to processor) issued by the European Commission on 4 June 2021 (2021/914) (as referenced in section 1 of Annex 3 to this DP Schedule, as amended (where appropriate) by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for UK transfers of Personal Data dated 21 March 2022 (as referenced in section 2 of Annex 3) and/or the country specific provisions for Switzerland (as referenced in section 3 of Annex 3).
 - 1.7 “**Security Event Data**” means information related to security events which is collected during Secureworks’ provision of SaaS Solutions.
 - 1.8 “**Subprocessor**” means a third party engaged by Secureworks (including without limitation an Affiliate and/or subcontractor of Secureworks) in connection with the processing of Personal Data.
 - 1.9 “**UK**” means the United Kingdom of Great Britain and Northern Ireland.
2. **Description of processing:** Annex 1 to this DP Schedule sets out a description of the processing

activities to be undertaken as part of the SaaS Solutions to be provided under the MSSP Addendum and this DP Schedule.

3. **Compliance with laws:** the parties agree to comply with their respective obligations under Privacy Laws. In particular, MSSP shall require each Customer to warrant and represent in the applicable Customer Agreement (on its behalf and on behalf of each of its Affiliates where applicable) that it has obtained and will maintain all necessary authorizations and consents required to enable Secureworks to provide the SaaS Solutions and process the Personal Data pursuant to this DP Schedule and MSSP Addendum in accordance with Privacy Laws.
4. **Secureworks obligations**
 - 4.1 **Instructions:** MSSP represents that it is authorized by the Customer to give instructions to Secureworks on the processing of Personal Data on behalf of the Customer (“Instructions”). Secureworks shall process the Personal Data only in accordance with reasonable and lawful Instructions (unless otherwise required to do so by applicable law). MSSP hereby instructs Secureworks to process and transfer the Personal Data in order to provide the SaaS Solutions and comply with Secureworks’ rights and obligations under the MSSP Addendum and this DP Schedule. Any additional or alternate Instructions must be agreed in writing, including the costs (if any) associated with complying with such Instructions. Secureworks is not responsible for ensuring any Instructions it receives under this DP Schedule comply with applicable law (including without limitation Privacy Law) and it will not be in default for complying with such Instructions. However, if Secureworks is of the opinion that an Instruction infringes applicable Privacy Laws, Secureworks shall notify MSSP as soon as reasonably practicable, MSSP shall promptly notify the Customer and Secureworks shall not be required to comply with such Instruction.
 - 4.2 **Confidentiality:** Secureworks shall maintain the confidentiality of the Personal Data in accordance with the MSSP Addendum and shall require persons authorized to process the Personal Data (including its Subprocessors) to have committed to materially similar obligations of confidentiality.
 - 4.3 **Disclosures:** Secureworks may only disclose the Personal Data to third parties (including without limitation its Affiliates and Subprocessors) for the purpose of:
 - (a) complying with Instructions
 - (b) as required in connection with the SaaS Solutions and as permitted by the MSSP Addendum and/or this DP Schedule, and/or
 - (c) to the extent required to comply with Privacy Laws, or an order of any court, tribunal, regulator or government agency with competent jurisdiction to which Secureworks, its Affiliates and/or Subprocessors is subject.
 - 4.4 **Assisting with data subject rights:** Secureworks shall, as required in connection with the SaaS Solutions and to the extent reasonably practicable, assist with requests from data subjects and consumers exercising their rights under Privacy Laws (including without limitation the right of access, rectification and/or erasure) in respect of the Personal Data. Secureworks may charge MSSP for such assistance if the cost of assisting exceeds a nominal amount. Secureworks shall forward to MSSP, as soon as practicable, any data subject rights requests Secureworks receives from relevant data subjects.
 - 4.5 **Security:** Taking into account industry standards, the costs of implementation, the nature, scope, context and purposes of the processing and any other relevant circumstances Secureworks shall implement the measures required by GDPR Article 32 (or similar provision under other applicable Privacy Laws). The parties agree that the security measures described in Annex 2 (Security Measures) provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause.
 - 4.6 **Subprocessors:** Secureworks is authorised under this DP Schedule to appoint and use Subprocessors (which are identified on the subprocessor list posted by Secureworks on its customer portal or the SaaS Solutions portal, as updated from time to time) to process the Personal Data in connection with the SaaS Solutions PROVIDED that Secureworks puts in place a contract in writing with each Subprocessor that imposes obligations that are (a) relevant to the services to be provided by the Subprocessors and (b) materially similar to the rights and/or obligations granted or imposed on Secureworks under this DP Schedule. If Secureworks proposes to appoint a new Subprocessor, Secureworks shall notify MSSP (including without limitation by email or by posting a notification on the customer portal or the SaaS Solutions portal) and allow MSSP to object to such appointment within thirty (30) days of such notification being made. MSSP may only object to the appointment of a new Subprocessor on reasonable data

protection related grounds. If MSSP objects, the parties shall use reasonable endeavours to agree alternative arrangements. If the parties cannot agree then MSSP may terminate the SaaS Solutions affected by the appointment of the new Subprocessor subject to providing thirty (30) days written notice to Secureworks and making payment to Secureworks of any and all fees that are due and owing for any SaaS Solutions supplied prior to the termination date (on payment terms in accordance with the Agreement). The parties may agree a shorter period of notice if applicable. Failure by MSSP to object to Secureworks' notification within thirty (30) days from the notification being made will be deemed to be MSSP's agreement to the addition of the new Subprocessor.

- 4.7 **Deletion of Personal Data:** Upon termination of the SaaS Solutions (for any reason) and if requested by MSSP in writing, Secureworks shall as soon as reasonably practicable delete the Personal Data, PROVIDED that Secureworks may: (a) retain one copy of the Personal Data as necessary to comply with any legal, regulatory, judicial, audit or internal compliance requirements; and/or (b) defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof cannot reasonably and practically be expunged from Secureworks' systems. The provisions of this DP Schedule shall continue to apply to Personal Data that is retained by Secureworks pursuant to this clause. For the purpose of (i) the SCCs Module Three, Clause 8.5 (Duration of processing and erasure or return of data) and (ii) the SCCs Modules One and Three, Clause 16(d) (Non-compliance with the Clauses and termination), upon termination (for any reason) of the SaaS Solutions, the Personal Data shall be deleted (and not returned to MSSP or Customer) and Secureworks shall only be required to certify the deletion of the Personal Data if requested in writing by MSSP.
- 4.8 **Demonstrating compliance:** Secureworks shall, upon reasonable prior written request from MSSP (such request not to be made more frequently than once in any twelve-month period), provide to MSSP such information as may be reasonably necessary to demonstrate Secureworks' compliance with its obligations under this DP Schedule.
- 4.9 **Audits and inspections:** Where MSSP reasonably believes the information provided under clause 4.8 above is not sufficient to demonstrate Secureworks' compliance with this DP Schedule, MSSP may request reasonable access to Secureworks' relevant processing activities in order to audit and/or inspect Secureworks' compliance with this DP Schedule PROVIDED THAT:
- (a) MSSP gives Secureworks reasonable prior written notice of at least thirty (30) days before any audit or inspection (unless a shorter notice period is required by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties or in the event of a Data Breach)
 - (b) audits or inspections may not be carried out more frequently than once in any twelve-month period (unless required more frequently by Privacy Laws, an order of a supervisory authority, otherwise agreed between the parties or in the event of a Data Breach)
 - (c) MSSP submits to Secureworks a detailed audit plan at least two (2) weeks in advance of the proposed audit date describing the proposed scope, duration and start date of the audit. Secureworks shall review the audit plan and provide MSSP with any material concerns or questions without undue delay. The parties shall then reasonably cooperate to agree a final audit plan
 - (d) Secureworks may restrict access to information in order to avoid compromising a continuing investigation, violating law or violating confidentiality obligations to third parties. Any access to sensitive or restricted facilities by MSSP is strictly prohibited due to regulatory restrictions on access to other customers' data, although MSSP and/or its auditor shall be entitled to observe the security operations center via a viewing window. MSSP shall not (and must ensure that its auditor shall not) allow any sensitive documents and/or details regarding Secureworks' policies, controls and/or procedures to leave the Secureworks location at which the audit or inspection is taking place (whether in electronic or physical form)
 - (e) MSSP carries out the audit or inspection during normal business hours and without creating a business interruption to Secureworks
 - (f) the audit or inspection is carried out in compliance with Secureworks' relevant on-site policies and procedures

- (g) where the audit is carried out by a third party on behalf of the MSSP, such third party is bound by similar obligations of confidentiality to those set out in the MSSP Addendum and is not a direct competitor of Secureworks. Secureworks reserves the right to require any such third party to execute a confidentiality agreement directly with Secureworks prior to the commencement of an audit or inspection, and
- (h) except where the audit or inspection discloses a failure on the part of Secureworks to comply with its material obligations under this DP Schedule, MSSP shall pay all reasonable costs and expenses (including without limitation any charges for the time engaged by Secureworks, its personnel and professional advisers) incurred by Secureworks in complying with this clause 4.9.

MSSP shall provide to Secureworks a copy of any audit reports generated in connection with an audit carried out under this clause 4.9, unless prohibited by applicable law. MSSP may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of applicable Privacy Laws. The audit reports shall be Confidential Information of the parties.

For the purpose of the SCCs, Module Three, Clauses 8.9(d) and (f) the parties agree that the provisions of clause 4.9 of the DP Schedule shall be incorporated into any audit request.

5. International transfers

- 5.1 Secureworks may, in connection with the provision of the SaaS Solutions, or in the normal course of business, make international transfers of the Personal Data and Security Event Data to its Affiliates and/or Subprocessors subject to the terms of this clause 5. Secureworks takes into consideration the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- 5.2 Where the provision of the SaaS Solutions and/or Secureworks' processing of Security Event Data involve a transfer of personal data from (a) the European Economic Area ("EEA"), the UK and/or Switzerland to (b) Secureworks (or any of Secureworks' Affiliates and/or Subprocessors) located in a Third Country (as defined below), the parties agree that the SCCs as referenced in Annex 3 to this DP Schedule shall apply to such transfer (as amended (where applicable) by the country specific provisions also referenced in Annex 3 for transfers from the UK and/or Switzerland). "Third Country" in this clause means a country that is not subject to an adequacy decision pursuant to Article 45 of the GDPR (or a similar provision in the Privacy Laws of the United Kingdom and/or Switzerland) and to which a transfer of personal data would be restricted or prohibited by Privacy Laws. In the event of a conflict the order of priority shall be (1) the SCCs, (2) this DP Schedule (3) the MSSP Addendum.
- 5.3 If the SCCs cease to provide a valid legal basis for the transfer of personal data, the parties shall without undue delay meet to agree in good faith what alternative transfer methods are available to ensure such transfers can continue in accordance with applicable Privacy Law and implement an agreed alternative method as soon as reasonably practicable. This may include the parties agreeing to enter into an alternative data transfer method where available and appropriate. The sole and exclusive remedy for failure to agree an alternative transfer method in accordance with this clause 5.3 shall be the termination of the affected SaaS Solutions. In such circumstances MSSP shall remain liable to pay to Secureworks all unpaid SaaS Solutions fees as set forth in the relevant Order accrued as of, and attributable to the period prior to, such termination together with any applicable fees associated with third party products or services.
- 5.4 The parties agree that where the SCCs require the use of best efforts in respect to a specific provision this shall be interpreted to mean an obligation on the relevant party to act in good faith, in a diligent, determined, prudent and reasonable manner, as if that party were seeking to achieve the result of that provision for its own benefit.

6. Data Breaches: Where a Data Breach is caused by Secureworks' failure to comply with its obligations under this DP Schedule, Secureworks shall:

- 6.1 notify MSSP without undue delay after establishing the occurrence of the Data Breach and shall, to the extent such information is known or available to Secureworks at the time, provide MSSP with details of the Data Breach, a point of contact and the measures taken or to be taken to address the Data Breach; and
- 6.2 reasonably cooperate and assist MSSP with any investigation into, and/or remediation of, the Data Breach (including, without limitation and where required by Privacy Laws, the provision of

notices to regulators and affected individuals).

In the event Customer intends to issue a notification regarding the Data Breach to a supervisory authority, other regulator, or law enforcement agency, MSSP will use all reasonable efforts to (a) obtain and share with Secureworks a copy of such notification (unless prohibited by applicable law) and (b) forward to Customer any comments made by Secureworks in relation to the notification together with a request for Customer to have due regard to such comments.

7. **Security Event Data:** MSSP will notify Customers (including as part of each Customer Agreement) about Secureworks' use of Security Event Data as described in this clause 7. Secureworks processes Security Event Data as part of its provision of SaaS Solutions. Customer acknowledges that Security Event Data may also be processed in order to develop, enhance and/or improve security services and the products and services offered and provided to customers. Secureworks shall be the controller in respect of any personal data in the Security Event Data and, as such, is responsible for processing the Security Event Data in accordance with applicable Privacy Laws. Restrictions on the processing, disclosure and transfer of Personal Data in this DP Schedule shall not apply to Security Event Data processed for the purposes described in this clause, PROVIDED THAT Secureworks shall not disclose any Security Event Data that is traceable to a Customer to any third parties (other than Affiliates and Subprocessors) unless permitted under this DP Schedule and/or the MSSP Addendum, or the disclosure is required in order to comply with applicable law or legal process. Secureworks shall not be required by MSSP or any Customer to return or delete Security Event Data upon termination of the SaaS Solutions (for any reason). If Customer is compelled by a legally binding order (e.g. of a court or regulatory authority of competent jurisdiction) to have the Security Event Data deleted, then Secureworks agrees, as legally required, to delete the Security Event Data that is the subject of the binding order as soon as practicable following receipt of a certified copy of such binding order.
8. **Privacy Impact Assessments:** Secureworks shall provide reasonable cooperation and assistance to MSSP, to the extent applicable in relation to Secureworks' processing of the Personal Data and within the scope of the agreed SaaS Solutions, in connection with any data protection impact assessment(s) which may be required in relation to the processing of Personal Data to be undertaken by Secureworks, including any required prior consultation(s) with supervisory authorities. Secureworks reserves the right to charge MSSP a reasonable fee for the provision of such cooperation and assistance.
9. **CCPA-Specific Requirements:** To the extent that Personal Data of California residents is processed in the provision of the SaaS Solutions, this clause 9 shall apply. Secureworks understands and agrees that it is expressly prohibited from retaining, using, or disclosing Personal Data of consumers for any purpose, including retaining, using, or disclosing such Personal Data of consumers for a commercial purpose, other than for a business purpose, including providing the SaaS Solutions or as expressly permitted in this DP Schedule or the MSSP Addendum. In addition, Secureworks shall not further collect, sell, or use Personal Data of consumers except as necessary to perform a business purpose, including to provide the SaaS Solutions or as expressly permitted in this DP Schedule or the MSSP Addendum. Secureworks certifies that it understands the restrictions contained in this clause and otherwise in this DP Schedule with respect to handling of Personal Data of consumers and shall comply with all such obligations. The parties expressly acknowledge and agree that no Personal Data of consumers is being provided to Secureworks for monetary or any other valuable consideration.
10. **General:** Notwithstanding anything in this DP Schedule or otherwise to the contrary, the parties agree that Secureworks' liability with respect to its processing of Personal Data under this DP Schedule (including without limitation the SCCs) shall be limited to the amounts and types of liability as set forth in the MSSP Addendum and the Agreement and nothing in this DP Schedule shall expand any responsibility, liability or obligation to pay damages, costs, expenses or otherwise beyond that set forth in the MSSP Addendum and the Agreement.
11. **Customer Agreement provisions:** MSSP warrants and represents the following: (i) it is authorised to act on behalf of the Customer in relation to any instructions, authorisations or other confirmations given under this DP Schedule; and (ii) it shall include in each executed Customer Agreement contractual provisions that are materially equivalent to those set out in this DP Schedule with the aim of giving full effect to the provisions agreed between the parties hereunder.

Annex 1 to the DP Schedule – Processing description

1	Subject matter and purpose	
	Subject to the terms of the MSSP Addendum, Secureworks provides information security services and processes the Personal Data for the purpose of providing such services as set out in the MSSP Addendum, applicable Order and applicable service level agreements, service descriptions or otherwise.	
2	Duration of processing	
	Secureworks retains and processes the Personal Data for the term of the MSSP Addendum and in accordance with the provisions of this DP Schedule regarding the return or deletion of the Personal Data.	
3	Categories of data subjects	
	The Personal Data processed and transferred may concern the following categories of data subjects: past, present and prospective (i) employees and partners, (ii) clients and individuals who use and access Customer information technology systems for which Secureworks provides SaaS Solutions, (iii) advisors, consultants, contractors, subcontractors and agents; and (iv) complainants, correspondents and enquirers, and (v) threat actors (suspected or confirmed).	
4	Categories of personal data	
	<p>4.1 When Secureworks is acting as a processor: the type of Personal Data that may be processed and/or transferred includes (without limitation):</p> <ul style="list-style-type: none"> (i) Network data (such as IP address, process name, process owner ID, user ID, MAC address or other unique device identifiers, network traffic flows, communications metadata, machine names) within process security logs or alerts; (ii) User authentication data (user ID, IP address, MAC address) and process activity (user ID, IP address, MAC address) in connection with endpoint agent activity; (iii) Any Personal Data within malicious file fragments, network fragments within process security logs or alerts; (iv) Any Personal Data which MSSP or Customer elects to include in the course of requesting customer support in the course of the provision of SaaS Solutions. <p>4.2 When Secureworks is acting as a controller: the type of personal data that may be processed and transferred may include (without limitation):</p> <ul style="list-style-type: none"> (i) the same information as set out in the preceding section 4.1(i)-(iii); (ii) any other information related to Security Event Data which is collected during Secureworks' provision of SaaS Solutions, and (iii) any personal data submitted through the use of the platform(s) supporting the SaaS Solutions, which may include (without limitation): (i) user ID in connection with analytics activities (browsing history) and/or (ii) user authentication data (first/last name, title/position, company, email, phone, physical business address, username, user ID) in connection with administering accounts. 	
5	Sensitive data	
	Special categories of personal data are not actively or intentionally collected. Safeguards and restrictions to protect any special categories of personal data that may be collected are as set out in Annex 2 (Security Measures).	
6	Nature of the processing	
	Personal data will be subject to the following processing activities: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	
7	Retention period	
	Retention periods are as set out in Secureworks' retention policy. The retention policy for specific SaaS Solutions is available upon written request.	
8	Contact details	
	8.1 MSSP contact details and Data Protection Officer	As set out in (or otherwise notified under) the MSSP Addendum
	8.2 Secureworks contact details and Data Protection Officer	Contact email: legal@secureworks.com DPO: privacy@secureworks.com

Annex 2 to the DP Schedule – Security Measures

This information security overview applies to Secureworks' corporate controls for safeguarding personal data.

Security Practices

Secureworks has implemented corporate information security practices and standards that are designed to safeguard Secureworks' corporate environment and to address:

(1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by Secureworks' executive management and undergo a formal review on an annual basis.

Organizational Security

It is the responsibility of the individuals across the organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, the function of information security provides:

1. Strategy and compliance with policies/standards and regulations, awareness and education, risk assessments and management, contract security requirements management, application and infrastructure consulting, assurance testing and drives the security direction of the company;
2. Security testing, design and implementation of security solutions to enable security controls adoption across the environment;
3. Security operations of implemented security solutions, the environment and assets, and manage incident response;
4. Forensic investigations with security operations, legal, data protection and human resources for investigations including eDiscovery and eForensics.

Asset Classification and Control

Secureworks' practice is to track and manage physical and logical assets. Examples of the assets that Secureworks IT might track include:

- Information Assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, archived information;
- Software Assets, such as identified applications and system software;
- Physical Assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These may include controls such as access management, encryption, logging and monitoring, and data destruction.

Personnel Security

As part of the employment process and subject to local law, employees undergo a screening process at hire and periodically thereafter. Secureworks' annual compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions.

Physical and Environmental Security

Secureworks uses a number of technological and operational approaches in its physical security program in regards to risk mitigation. Secureworks' security team works closely with each site to determine appropriate measures are in place and continually monitor any changes to the physical infrastructure, business, and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniquenesses in business practice and expectations of Secureworks as a whole. Secureworks balances its approach towards security by considering elements of control that include architecture, operations, and systems.

Communications and Operations Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program which may include testing, business impact analysis and management approval where appropriate. Incident response procedures exist for security and data protection incidents which may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

To protect against malicious use of assets and malicious software, additional controls may be implemented based on risk. Such controls may include, but are not limited to, information security policies and standards, restricted access, designated development and test environments, virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans, intrusion prevention monitoring and response, logging and

alerting on key events, information handling procedures based on data type, e-commerce application and network security, and system and application vulnerability scanning.

Access Controls

Access to corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on least privileges. Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Secureworks environment. Based on risk to Secureworks' business and customers, there are pre-determined timeframes for remediation. In addition, vulnerability scanning and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, privacy and compliance departments work to identify regional laws and regulations applicable to Secureworks. These requirements cover areas such as, intellectual property of the company and our customers, software licenses, protection of employee and customer personal data, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements. Mechanisms such as the information security program, the executive risk committee, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security awareness, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

Annex 3 to the DP Schedule

STANDARD CONTRACTUAL CLAUSES
(Module One: controller to controller and Module Three: processor to processor)

In the event of a transfer from the EEA, the UK and/or Switzerland to a Third Country (as defined in clause 5.2 above) in accordance with the DP Schedule, such transfer shall be subject to the terms of this Annex 3 and the SCCs set out below shall apply and be incorporated by reference into, and form part of, this DP Schedule.

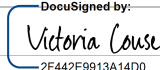
1. **Transfers from the EEA**

- 1.1 In relation to transfers of personal data that are subject to the Privacy Laws of a country within the EEA: Module One and Module Three of the SCCs shall apply as set out below.

For SCCs Module One (controller to controller) AND Module Three (processor to processor):	
Clause 7 (Docking clause)	The optional docking clause shall apply.
Clause 11(a) (Redress)	The optional wording in Clause 11(a) shall not apply.
Clause 13 (Supervision) and Annex I.C	All the options in Clause 13(a) are retained and shall apply depending on the establishment of the data exporter (as identified by the data exporter's address set out in, or otherwise notified under, the MSSP Addendum).
Clause 17 (Governing law)	Option1: The SCCs shall be governed by the law of the country in which the data exporter is established provided such law allows for third-party beneficiary rights. Where such law does not allow for third-party beneficiary rights, the SCCs shall be governed by Irish law.
Clause 18(b) (Choice of forum and jurisdiction)	The court of the country in which the data exporter is established.
For SCCs Module Three (processor to processor) ONLY:	
Clause 9(b) (Use of sub-processors)	Option 2: General written authorisation is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least thirty (30) days in advance.

- 1.2 The Appendix to the SCCs is completed as set out below for both Module One (controller to controller) and Module Three (processor to processor):

Annex I.A (List of parties)	
Data exporter name and address:	The data exporter is the MSSP as defined in the MSSP Addendum
Data importer name and address:	The data importer is Secureworks Inc. and its address is One Concourse Parkway, Atlanta, GA 30328, US.
Activities relevant to the data transferred:	Activities relate to the provision by data importer to data exporter (and Customers of data exporter) of information security services (as set out in the MSSP Addendum and Agreement)
Role of data exporter:	(1) Module One: the data exporter is entering into Module One as agent for and on behalf of its Customers (who are the controllers) (2) Module Three: the data exporter is a processor
Role of data importer:	(1) Module One: the data importer is a controller in respect of any personal data contained in Security Event Data (2) Module Three: the data importer is a processor
Signature by data exporter:	(1) Module One: Acceptance by the MSSP of the MSSP Addendum after the date of publication thereof will be deemed to be execution of Module One of the SCCs by the MSSP acting for and on behalf of its Customers as their authorised representative and MSSP

	hereby confirms that it has the necessary authority to act on behalf of its Customer(s); and (2) Module Three : Acceptance by the MSSP of the MSSP Addendum after the date of publication thereof will be deemed to be execution by the MSSP of Module Three of the SCCs.
Signature by data importer:	 2F442E9913A14D0...
The remainder of this Annex I.A shall be deemed completed with the information set out in Annex 1 of the DP Schedule (and, where applicable, any other information set out in the DP Schedule and/or the MSSP Addendum and Agreement)	
Annex I.B (Description of transfer)	
B1	Categories of data subjects whose personal data is transferred: shall be completed with the information set out in section 3 of Annex 1 to the DP Schedule.
B2	Categories of personal data transferred: shall be completed with the information set out in section 4 of Annex 1 to the DP Schedule.
B3	Sensitive data transferred: shall be completed with the information set out in section 5 of Annex 1 to the DP Schedule.
B4	Frequency of the transfer: the transfer is made on a continuous basis in connection with the provision of SaaS Solutions.
B5	Nature of the processing: shall be completed with the information set out in section 6 of Annex 1 to the DP Schedule.
B6	Purpose of the data transfer and further processing: (i) for Module One (controller to controller) SCCs: data importer will transfer and further process the personal data (including Security Event Data) described in B2 for the purpose of: (a) developing, enhancing and/or improving its security services and the products and services it offers and provides to customers, (b) administration and management of data importer's products, services and customer accounts, and (c) research and analytics; (ii) for Module Three (processor to processor) SCCs: data importer will transfer and further process the personal data described in B2 for the purpose of (a) providing information security services and customer support (as set out in the MSSP Addendum and applicable Order, service level agreement, service descriptions or otherwise) and (b) enabling the data exporter to provide its Customers (who are the controllers of personal data) with SaaS Solutions.
B7	Period of time for which personal data will be retained: shall be completed with the information set out in section 7 of Annex 1 to the DP Schedule.
B8	For transfers to subprocessors: the subject matter, nature and duration of processing by subprocessors acting on behalf of data importer will be the same as for data importer.
Annex I.C	
The competent supervisory authority/ies will be those located in the country in which the data exporter is located (as identified by the data exporter's address set out in, or otherwise notified under, the MSSP Addendum).	
Annex II (Security measures)	
The description of the technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons are as set out in Annex 2 (Security Measures) to the DP Schedule.	

2. Transfers from the UK

- 2.1 For transfers of personal data that are subject to UK Privacy Laws: the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses for UK transfers of Personal Data dated 21 March 2022 ("**Addendum**") (as amended or updated from time to time) issued by the UK Information

Commissioner shall apply and be incorporated by reference into, and form part of, this DP Schedule, and shall come into effect, where applicable, upon signature by the parties as specified in section 1.2 of Annex 3 to the DP Schedule. Capitalised terms used in this section 2 that are not defined in the DP Schedule shall have the meaning set out in the Addendum.

2.2 The Tables in the Addendum shall be completed as follows:

Table 1: Parties		
Start date	Upon signature by the parties as specified in section 1.2 of Annex 3.	
The Parties	Exporter (who sends the Restricted Transfer):	Importer (who receives the Restricted Transfer):
	The data exporter is as defined in section 1.2 of Annex 3.	Secureworks Inc. (as specified in section 1.2 of Annex 3).
Parties' details and key contacts	As set out in section 8 of Annex 1 to the DP Schedule, or as otherwise notified between the parties from time to time.	
Signature	The Addendum shall be deemed signed by the parties as set out in section 1.2 of Annex 3.	
Table 2: Selected SCCs, Modules and Selected Clauses		
Addendum EU SCCs:	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:	
Module One:	<ul style="list-style-type: none"> – Clause 7 (Docking clause): the docking clause shall apply – Clause 11 (Redress): the optional wording in Clause 11(a) shall not apply 	
Module Three:	<ul style="list-style-type: none"> – Clause 7 (Docking clause): the docking clause shall apply; – Clause 11 (Redress): the optional wording in Clause 11(a) shall not apply; – Clause 9(b) (Sub-processors): Option 2: General written authorisation is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least thirty (30) days in advance. 	
Table 3: Appendix Information		
“ Appendix Information ” means the information which must be provided for the selected Modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for the Addendum is set out as follows:		
Annex I.A: List of Parties:	See section 1.2 of Annex 3.	
Annex I.B: Description of Transfer:	See section 1.2 of Annex 3.	
Annex II: Technical and organisational measures	See Annex 2 of the DP Schedule.	
Annex III: List of Sub processors:	See Clause 4.6 of the DP Schedule.	
Table 4: Ending this Addendum when the Approved Addendum changes		
Ending this Addendum when the Approved Addendum changes	Which Parties may end the Addendum (as set out in Section 19 of the Addendum): <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party	

3. **Transfers from Switzerland**

3.1 **Definitions** – in this section 3, the following definitions are used:

(a) “**FDPIC**” means the Federal Data Protection and Information Commissioner; and

(b) “**Swiss Data Protection Laws**” means any law, enactment, regulation or order in Switzerland concerning the processing of data relating to living persons, including, as applicable, the Federal Act on Data Protection of 19 June 1992 (SR 235.1) (“**FADP**”) and the revised version of the FADP dated 25 September 2020 (“**Revised FADP**”).

3.2 **SCCs** – For transfers from Switzerland to a Third Country of personal data that are subject to Swiss Data Protection Laws, the parties agree to:

- (a) adopt the GDPR standard for all such data transfers;
- (b) use Module One (controller to controller) and Module Three (processor to processor) of the SCCs; and
- (c) amend the SCCs in order to comply with Swiss Data Protection Laws as set out below.

3.3 **Amendments to the SCCs** – Where the SCCs apply (in accordance with section 3.2 above) and the transfer from Switzerland to a Third Country is:

- (a) exclusively subject to Swiss Data Protection Laws, OR
- (b) subject to both Swiss Data Protection Laws and the GDPR

the following amendments shall apply:

- (i) references in the SCCs to “Regulation (EU) 2016/679” or “that Regulation” are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented by references to the “FADP and Revised FADP, as appropriate” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced or supplement (as applicable) with the equivalent Article or Section of the FADP or Revised FADP;
- (ii) reference to the “EU”, “EU Member State”, “European Union” and “Union” are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented with references to “Switzerland”; and
- (iii) references to competent supervisory authority are (in respect of section 3.3(a) above) replaced or (in respect of section 3.3(b) above) supplemented with references to FDPIC.

3.4 In addition to the above, the following amendments shall also apply to the SCCs:

Swiss amendments that apply to Module One (controller to controller) AND Module Three (processor to processor) SCCs:	
Clause 7 (Docking clause)	The optional docking clause shall apply.
Clause 11(a) (Redress)	The optional wording in Clause 11(a) shall not apply.
Clause 13 (Supervision) and Annex I.C	<ul style="list-style-type: none"> – Where the transfer is exclusively subject to Swiss Data Protection Laws: FDPIC. – Where the transfer is subject to both Swiss Data Protection Laws and GDPR: <ol style="list-style-type: none"> (i) FDPIC is the supervisory authority insofar as the transfer is governed by Swiss Data Protection Laws; and (ii) the EU authority is the supervisory authority insofar as the data transfer is governed by the GDPR (the criteria of Clause 13(a) for the selection of the competent authority must be observed).
Clause 17 (Governing law)	<ul style="list-style-type: none"> – Where the transfer is exclusively subject to Swiss Data Protection Laws: Swiss law is the governing law. – Where the transfer is subject to both Swiss Data Protection Laws and GDPR: the law of the country in which the data exporter is established will apply provided such law allows for third-party beneficiary rights. Where such law does not allow for third-party beneficiary rights, the SCCs shall be governed by Irish law.
Clause 18(b) (Choice of forum and jurisdiction)	<ul style="list-style-type: none"> – Clause 18(b): The courts of the country in which the data exporter is established – Clause 18(c): The term “Member State” in the SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs.
Annex I.A	For a list of the parties see section 1.2 of Annex 3.
Annex I.B	For a description of the transfer see section 1.2 of Annex 3.

Annex II	For the technical and organisational measures see Annex 2.
Swiss amendments to ONLY Module Three (processor to processor) SCCs:	
Clause 9(b) (Use of sub-processors)	Option 2: General written authorisation is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least thirty (30) days in advance.

- 3.5 **Supplemental** – The SCCs shall protect the data of legal entities in Switzerland until the entry into force of the Revised FADP.
- 3.6 **Incorporation** – The SCCs (Module One and Module Three) adapted for Switzerland in accordance with this section 3 shall apply and shall be incorporated by reference into, and form part of, this DP Schedule and will come into effect, where applicable, upon signature by the parties in accordance with section 1.2 of Annex 3.