Secureworks

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") forms part of the CRA between the Customer and Secureworks and except as expressly stated applies solely where Secureworks processes Personal Data (as defined below) as a processor for the Customer in the provision of Services. Except as otherwise expressly stated, Customer is the controller and Secureworks is the processor (as defined below) of the Personal Data processed under this CRA. In the event of a conflict between this DPA and the CRA, this DPA shall control with respect to its subject matter.

1. **Definitions**: References in this DPA to "**controller**", "**data subject**", "**processor**", "**processing**" (and its derivatives) and "**supervisory authority**" shall have the meanings ascribed to them under Privacy Laws. Capitalized terms not defined in this DPA shall have the meaning set out in the CRA. In this DPA:

   1.1 "**Data Breach**" means an actual breach by Secureworks of the security obligations under this DPA leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise processed.

   1.2 "**Personal Data**" means any information relating to an identified or identifiable natural person which is processed by Secureworks, acting as a processor on behalf of the Customer, in the provision of the Services.

   1.3 "**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 CRA is subject and which are applicable to the Services including, without limitation, the General Data Protection Regulation 2016/679 (the "**GDPR**").

   1.4 "**Security Event Data**" means information related to security events which is collected during Secureworks' provision of services.

   1.5 "**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.

2. **Description of processing**: a description of the processing activities to be undertaken as part of the CRA and this DPA is set out in Annex 1.

3. **Compliance with laws**: the parties agree to comply with their respective obligations under Privacy Laws. In particular, Customer warrants and represents (on its behalf and on behalf of each of its Affiliates where applicable) that (i) it has obtained and will maintain all necessary authorizations and consents required to enable Secureworks to provide the Services and process the Personal Data pursuant to this DPA and CRA in accordance with the Privacy Laws and (ii) it shall provide all necessary authorizations and consents to Secureworks personnel whose personal data is processed by Customer in the course of providing Services to Customer.

4. **Secureworks obligations**

   4.1 **Instructions:** Secureworks shall process the Personal Data only in accordance with Customer's reasonable and lawful instructions (unless otherwise required to do so by applicable law). Customer hereby instructs Secureworks to process the Personal Data to provide the Services and comply with Secureworks' rights and obligations under the CRA and this DPA. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Customer is solely responsible for ensuring its instructions comply with applicable law and is solely responsible for the consequences of Secureworks complying with them and Secureworks shall not be in default by doing so. However, if Secureworks is of the opinion that a Customer instruction infringes applicable Privacy Laws, Secureworks shall notify Customer as soon as reasonably practicable and shall not be required to comply with such instruction.

   4.2 **Confidentiality**: To the extent the Personal Data is confidential (pursuant to applicable law), Secureworks shall maintain the confidentiality of the Personal Data in accordance with the CRA 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 Customer's reasonable and lawful instructions

      (b) as required in connection with the Services and as permitted by the CRA and/or this DPA, 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 Services and to the extent reasonably practicable, assist Customer to respond to requests from data subjects 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 Customer for such assistance if the cost of assisting exceeds a nominal amount. Secureworks shall forward to Customer as soon as practicable any data subject rights requests Secureworks receives from Customer's 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. The parties agree that the security measures described in Annex 2 (Information Security Measures) provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause.

   4.6 **Subprocessors**: Customer agrees that Secureworks may appoint and use Subprocessors (which are identified on the subprocessor list posted on the customer portal or the Cloud Services portal, as updated from time to time) to process the Personal Data in connection with the Services PROVIDED that Secureworks puts in place a contract in writing with each

Subprocessor that imposes obligations that are (i) relevant to the services to be provided by the Subprocessors and (ii) materially similar to the rights and/or obligations granted or imposed on Secureworks under this DPA.

4.7 **Deletion of Personal Data:** Upon termination of the Services (for any reason) and if requested by Customer 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 DPA shall continue to apply to Personal Data that is retained by Secureworks pursuant to this clause. Secureworks reserves the right to charge Customer for any reasonable costs and expenses incurred by Secureworks in deleting the Personal Data pursuant to this clause.

4.8 **Demonstrating compliance**: Secureworks shall, upon reasonable prior written request from Customer (such request not to be made more frequently than once in any twelve-month period), provide to Customer such information as may be reasonably necessary to demonstrate Secureworks' compliance with its obligations under this DPA.

4.9 **Audits and inspections**: Where Customer reasonably believes the information provided under clause 4.8 above is not sufficient to demonstrate Secureworks' compliance with this DPA, Customer may request reasonable access to Secureworks' relevant processing activities in order to audit and/or inspect Secureworks' compliance with this DPA PROVIDED THAT:

(a) Customer 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) Customer submits to Secureworks a detailed audit plan at least two 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 Customer with any material concerns or questions without undue delay. The parties will 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 Customer is strictly prohibited due to regulatory restrictions on access to other customers' data, although Customer and/or its auditor shall be entitled to observe the security operations center via a viewing window). Customer 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) Customer 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 Customer, such third party is bound by similar obligations to those set out in the CRA 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 DPA, Customer 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.

Customer shall provide to Secureworks a copy of any audit reports generated in connection with an audit carried out under this clause, unless prohibited by applicable law. Customer 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.

5. **International transfers**: Secureworks may, in connection with the provision of the Services, or in the normal course of business, make international transfers of the Personal Data to its Affiliates and/or Subprocessors. Where the provision of Services involves the transfer of Personal Data from countries within the European Economic Area ("EEA") to countries outside the EEA (which are not subject to an adequacy decision under Directive 95/46/EC or the GDPR) such transfer shall be subject to:

5.1 Secureworks has implemented appropriate security measures to adequately protect the transfer of such Personal Data

5.2 Secureworks having in place intra-group agreements with any Affiliates which may have access to the Personal Data, such agreements incorporating the applicable EU Commission approved Standard Contractual Clauses ("**Standard Contractual Clauses**"); and

5.3 Secureworks having in place agreements with its relevant Subprocessors that incorporate the applicable Standard Contractual Clauses (as appropriate).

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

6.1 notify Customer 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 Customer with details of the Data Breach, a point of contact and the measures taken or to be taken to address the Data Breach

6.2 reasonably cooperate and assist Customer 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, law enforcement agency, Customer shall (unless prohibited by law) allow Secureworks to review the notification and Customer shall have due regard to any reasonable comments or amendments proposed by Secureworks.

7. **Security Event Data**: Secureworks will process Security Event Data as part of its provision of Services. Customer acknowledges that Secureworks may also process Security Event Data in order to develop, enhance and/or improve its security services and the products and services it offers and provides 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 disclosure and transfer of Personal Data in this DPA shall not apply in connection with Secureworks' processing such Security Event Data for the purposes described in this clause, however, Secureworks shall not disclose any Security Event Data that is traceable to Customer to any third parties (other than Affiliates and Subprocessors) unless permitted under this CRA and/or the DPA, or the disclosure is required in order to comply with applicable law or legal process. Secureworks shall not be required to return or delete Security Event Data upon termination of the Services (for any reason). Customer shall ensure its personnel and any other data subjects whose personal data is processed by Secureworks in connection with the Services are appropriately notified of the fact their personal data may be processed in connection with the development, enhancement and/or provision of Secureworks' products or services as described in this clause. 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 appropriate, to anonymize, pseudonymize or 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 Customer, to the extent applicable in relation to Secureworks' processing of the Personal Data and within the scope of the agreed Services, in connection with any data protection impact assessment(s) which the Customer may carry out 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 Customer a reasonable fee for the provision of such cooperation and assistance.

Annex 1 – Processing description

Subject matter and purpose	Subject to the terms of the CRA, Secureworks provides information security services for the Customer and processes the Personal Data for the purpose of providing such services as set out in applicable Transaction Document, service level agreements, Service descriptions or otherwise
Duration of processing	Secureworks will retain and process the Personal Data for the term of the CRA and in accordance with the provisions of this DPA regarding the return or deletion of the Personal Data
Data subjects	The Personal Data 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 services, (iii) advisors, consultants, contractors, subcontractors and agents; and (iv) complainants, correspondents and enquirers
Type of personal data	For both the Cloud and MSS Services: Personal Data may be contained: 1. within the security logs or alerts which may include information related to IT resources access, such as user name, identification number, location, IP address, MAC address or other device identifier, resource accessed, time of access and device name; 2. within context related to the security logs or alert which may include malicious files, network fragment, process details, domain name, network connections; and 3. within the user account created to access Secureworks Cloud or MSS resources (e.g. customer portal access). For SRC (Consulting) Services: Personal Data which may be processed by Secureworks if necessary for the provision of the Consulting Services may include any or all of the following: 1. contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information); 2. employment details (which may include company name, job title, grade, demographic and location data); 3. IT systems information (which may include user ID and password, computer name, domain name, IP address, and software usage pattern tracking information i.e. cookies); 4. data subject's e-mail content and transmission data which is available on an incidental basis for the provision of information technology consultancy, support and services (incidental access may include accessing the content of e-mail communications and data relating to the sending, routing and delivery of e-mails); 5. details of goods or services provided to or for the benefit of data subjects; 6. financial details (e.g. credit, payment and bank details) 7. special categories of data (if appropriate) which may involve the incidental processing of personal data which may reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data and biometric data for the purpose of uniquely identifying a natural person; data concerning health (including physical or mental health or condition); sexual life or sexual orientation; criminal offences or alleged offences and any related court proceedings; social security files.

Annex 2 – Information Security Measures

This information security overview applies to Secureworks' corporate controls for safeguarding Customer 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, 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 information, 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.