

## DATA PROTECTION ADDENDUM

This Data Protection Addendum (“**DPA**”) and the SCCs (as defined below), if applicable, are incorporated by reference into and form part of the CRA. Except as expressly stated, this DPA applies solely where Secureworks processes Personal Data (as defined below) as a processor on behalf of the Customer in connection with 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 the 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**”, “**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**”). Capitalized terms not defined in this DPA shall have the meaning set out in the CRA. References in this DPA to Schedules are to the Schedules to this DPA. 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 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 on behalf of the Customer in anticipation of, in connection with or incidental to the performance of the CRA. 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.
  - 1.3 “**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 GDPR, the United Kingdom Data Protection Act 2018 (“**UK DPA**”), the UK GDPR (as defined in section 3 of the UK DPA), and the CCPA.
  - 1.4 “**SCCs**” or “**Standard Contractual Clauses**” means Module One (controller to controller) and Module Two (controller to processor) of the Standard Contractual Clauses issued by the European Commission on 4 June 2021 (2021/914) as referenced in Schedule 3, and 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 and/or the country specific provisions for Switzerland set out in Schedule 3.
  - 1.5 “**Security Event Data**” means information related to security events which is collected during Secureworks’ provision of Services.
  - 1.6 “**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**: Schedule 1 sets out a description of the processing activities to be undertaken as part of the Services to be provided under the CRA and this DPA.
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 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 Privacy Laws.
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 and transfer the Personal Data in order 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 (including without limitation Privacy Law) and is solely responsible for the consequences of Secureworks complying with such instructions 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**: 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 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 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 (or similar provision under other applicable Privacy Laws). The parties agree that the security measures described in Schedule 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**: 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 (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 DPA. If Secureworks proposes to appoint a new Subprocessor, Secureworks shall notify Customer (including without limitation by email or by posting a notification on the customer portal or the Cloud Services portal) and allow Customer to object to such appointment within 30 days of such notification being made. Customer may only object to the appointment of a new Subprocessor on reasonable data protection related grounds. If Customer objects, the parties shall use reasonable endeavours to agree alternative arrangements. If the parties cannot agree then Customer may terminate all Services 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 Services supplied prior to the termination date (on payment terms in accordance with the CRA). The parties may agree a shorter period of notice if applicable. Failure by Customer to object to Secureworks' notification within thirty (30) days from the notification being made will be deemed to be Customer's agreement to the addition of the new Subprocessor.
- 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. For the purpose of (i) the SCCs, Module Two, Clause 8.5 (*Duration of processing and erasure or return of data*) and (ii) the SCCs, Clause 16(d) (*Non-compliance with the Clauses and termination*), the Customer elects that upon termination (for any reason) of the Services or this DPA, the Personal Data will be deleted (and not returned to Customer) and Secureworks will only be required to certify the deletion of the Personal Data if requested in writing by Customer.
- 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 (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 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 of confidentiality 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 4.9.

Customer 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. 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.

For the purpose of the SCCs, Module Two, Clauses 8.9(c) and 8.9(d), Customer agrees that the provisions of clause 4.9 of the DPA shall be incorporated into any audit request made by the Customer.

5. **International transfers**

- 5.1 Secureworks may, in connection with the provision of the Services, 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 Services and/or Secureworks' processing of Security Event Data involve a transfer of personal data from (a) the European Economic Area, the United Kingdom 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 Schedule 3 shall apply to such transfer (as amended (where applicable) by the country specific provisions also referenced in Schedule 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 between the SCCs, this DPA or Privacy Law, the order of priority will be (1) Privacy Law, (2) the SCCs and (3) this DPA.
- 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 Services. In such circumstances Customer shall remain liable to pay to Secureworks all unpaid Services fees as set forth in the relevant Transaction Document accrued as of, and attributable to the period prior to, such termination together with any applicable fees associated with Third Party Products (as defined in the CRA).
- 5.4 The parties agree that where the SCCs require the use of best efforts in respect to a specific provision this will 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 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; and
- 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, or law enforcement agency, Customer shall (unless prohibited by applicable law) allow Secureworks to review the notification and Customer shall have due regard to any reasonable comments and/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 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 disclosure and transfer of Personal Data in this DPA 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 Customer to any third parties (other than Affiliates and Subprocessors) unless permitted under this DPA and/or the CRA, or the disclosure is required in order to comply with applicable law or legal process. Secureworks shall not be required by Customer to return or delete Security Event Data upon termination of the Services (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 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.
9. **CCPA-Specific Requirements:** To the extent that Personal Data of California residents is processed in the provision of the Services, 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 Services or as expressly permitted in this DPA or the CRA. In addition, Secureworks will not further collect, sell, or use Personal Data of consumers except as necessary to perform a business purpose, including to provide the Services or as expressly permitted in this DPA or the CRA. Secureworks certifies that it understands the restrictions contained in this clause and otherwise in this DPA with respect to handling of Personal Data of consumers and shall comply with all such obligations. The parties expressly acknowledge and agree that Customer is not providing any Personal Data of consumers to Secureworks for monetary or any other valuable consideration.
10. **General:** Notwithstanding anything in this DPA or otherwise to the contrary, the parties agree that Secureworks' liability with respect to the Personal Data processed by Secureworks on behalf of Customer under this DPA and under the SCCs shall be limited to the amounts and types of liability as set forth in the CRA and nothing in this DPA shall expand any responsibility, liability or obligation to pay damages, costs, expenses or otherwise beyond that set forth in the CRA.

**SCHEDULE 1 TO DATA PROTECTION ADDENDUM**  
**Processing description**

|          |   |
|----------|---|
| <b>1</b> | <p><b>Subject matter and purpose</b></p> <p>Subject to the terms of the CRA, Secureworks provides information security services for Customer and processes the Personal Data for the purpose of providing such services as set out in the applicable Transaction Document, service level agreements, Service descriptions or otherwise.</p>   |
| <b>2</b> | <p><b>Duration of processing</b></p> <p>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.</p>  |
| <b>3</b> | <p><b>Categories of data subjects</b></p> <p>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 Services, (iii) advisors, consultants, contractors, subcontractors and agents; (iv) complainants, correspondents and enquirers and (v) threat actors (suspected or confirmed).</p>   |
| <b>4</b> | <p><b>Categories of personal data</b></p> <p><b>4.1 When Secureworks is acting as a processor:</b> the type of Personal Data that may be processed and/or transferred includes (without limitation):</p> <p>(a) <b><u>For both Cloud and MSS Services:</u></b></p> <ul style="list-style-type: none"> <li>(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;</li> <li>(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;</li> <li>(iii) Any Personal Data within malicious file fragments, network fragments within process security logs or alerts;</li> <li>(iv) Any Personal Data which the Customer elects to include in the course of requesting customer support in the course of the provision of Services.</li> </ul> <p>(b) <b><u>For SRC (Consulting) Services:</u></b></p> <ul style="list-style-type: none"> <li>(i) contact details (which may include name, address, e-mail address, phone and fax contact details and associated local time zone information);</li> <li>(ii) employment details (which may include company name, job title, grade, demographic and location data);</li> <li>(iii) 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));</li> <li>(iv) data subjects' 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</li> </ul> |

|          |   |  |
|----------|---|--|
|          | <p>communications and data relating to the sending, routing and delivery of e-mails);</p> <p>(v) details of goods or services provided to or for the benefit of data subjects;</p> <p>(vi) financial details (e.g. credit, payment and bank details);</p> <p>(vii) 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.</p> <p><b>4.2 When Secureworks is acting as a controller:</b> the type of personal data that may be processed and transferred may include (without limitation):</p> <p>(i) the same information as set out in the preceding <b>section 4.1(a)(i)-(iv)</b>;</p> <p>(ii) any other information related to Security Event Data which is collected during Secureworks' provision of Services, and</p> <p>(iii) any personal data that Customer (or its personnel) may submit through the use of the platform(s) supporting the Services, 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.</p> |  |
| <b>5</b> | <p><b>Sensitive data</b></p> <p><b>5.1 When Secureworks is providing SRC (Consulting) Services and acting as a processor:</b> the provision of Services may involve the incidental processing of special categories of personal data as described in section 4.1(b)(vii) above.</p> <p><b>5.2 When Secureworks is acting as a controller:</b> special categories of personal data are not actively or intentionally collected.</p> <p>In each case, safeguards and restrictions to protect any special categories of personal data that may be collected are as set out in Schedule 2 (Security Measures).</p>  |  |
| <b>6</b> | <p><b>Nature of the processing</b></p> <p>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.</p>   |  |
| <b>7</b> | <p><b>Retention period</b></p> <p>Retention periods are as set out in Secureworks' retention policy. The retention policy for specific Services is available upon written request from Customer.</p>  |  |
| <b>8</b> | <p><b>Contact details</b></p>   |  |
|          | 8.1 <b>Customer</b> contact details and Data Protection Officer:  | As set out in (or otherwise notified under) the CRA  |
|          | 8.2 <b>Secureworks</b> contact details and Data Protection Officer:   | Contact email: <a href="mailto:legal@secureworks.com">legal@secureworks.com</a><br>DPO: <a href="mailto:privacy@secureworks.com">privacy@secureworks.com</a> |



## **SCHEDULE 2 TO DATA PROTECTION ADDENDUM**

### **Security Measures**

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

Published date: April 23, 2024

drive compliance with these requirements.

**SCHEDULE 3 TO DATA PROTECTION ADDENDUM**

**Standard Contractual Clauses**  
**(Module One: controller to controller and Module Two: controller to processor)**

In the event of a transfer from the European Economic Area (“**EEA**”), the UK and/or Switzerland to a Third Country (as defined in clause 5.2) in accordance with the DPA, such transfer shall be subject to the terms of this Schedule 3 and the Standard Contractual Clauses set out below shall apply and shall be incorporated by reference into, and form part of, this DPA.


**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 Two of the SCCs shall apply as set out below.

| <b>For SCCs Module One (controller to controller) AND Module Two (controller to processor):</b> |  |
|---|--|
| <b>Clause 7 (Docking clause)</b>  | The optional docking clause shall apply.   |
| <b>Clause 11(a) (Redress)</b>   | The optional wording in Clause 11(a) shall <b>not</b> apply.   |
| <b>Clause 13 (Supervision) and Annex I.C</b>  | 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 CRA).  |
| <b>Clause 17 (Governing law)</b>  | 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. |
| <b>Clause 18(b) (Choice of forum and jurisdiction)</b>  | The court of the country in which the data exporter is established.  |
| <b>For SCCs Module Two (controller to processor) ONLY:</b>                                      |  |
| <b>Clause 9(a) (Use of sub-processors)</b>  | <b>Option 2: General written authorisation</b> is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) 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 Two (controller to processor):

| <b>Annex I.A (List of parties)</b>     |   |
|--|---|
| <b>Data exporter name and address:</b> | The data exporter is:<br>(i) the Customer and/or Customer Affiliate that has entered into the Transaction Document and/or |

|   |   |
|---|---|
|   | <p>(ii) the relevant Customer Affiliate (if any) that is receiving Services (under the CRA) and is based in the EEA, the UK, and/or Switzerland ("<b>Relevant Affiliates</b>").</p> <p>The data exporter's address is the Customer's address or the Customer Affiliate's address as set out in the Transaction Document.</p>  |
| <b>Data importer name and address:</b>  | The data importer is Secureworks Inc. and its address is One Concourse Parkway, Atlanta, GA 30328, US.  |
| <b>Activities relevant to the data transferred:</b>   | Activities relate to the provision by data importer to data exporter of information security services (as set out in the applicable Transaction Document, service level agreement, Services description or otherwise).  |
| <b>Role of data exporter:</b>   | The data exporter is a <b>controller</b> .  |
| <b>Role of data importer:</b>   | <p>The data importer is:</p> <p>(i) a <b>processor</b> in respect of Personal Data (as defined in the DPA) and</p> <p>(ii) a <b>controller</b> in respect of any personal data contained in Security Event Data.</p>  |
| <b>Signature by data exporter:</b>  | <p>The SCCs shall be deemed to have been signed:</p> <p>(i) if the Customer and/or Customer Affiliate has signed an offline CRA, on the same date as such CRA is executed; or</p> <p>(ii) if the Customer and/or Customer Affiliate is trading under the online CRA, on the date of execution of the relevant Transaction Document.</p> <p>Where applicable, Customer enters into these Clauses for and on behalf of itself and each Relevant Affiliate and hereby confirms that it has the necessary authority to do so.</p> |
| <b>Signature by data importer:</b>  |   |
| The remainder of this Annex I.A shall be deemed completed with the information set out in Schedule 1 of the DPA (and, where applicable, any other information set out in the DPA and/or CRA). |   |
| <b>Annex I.B</b>  |   |
| <b>B1</b>   | Categories of data subjects whose personal data is transferred: shall be completed with the information set out in Schedule 1, section 3.   |
| <b>B2</b>   | Categories of personal data transferred: shall be completed with the information set out in Schedule 1, section 4.  |
| <b>B3</b>   | Sensitive data transferred: shall be completed with the information set out in Schedule 1, section 5.   |
| <b>B4</b>   | Frequency of the transfer: The transfer is made on a continuous basis for MSS and Cloud Services. For SRC (Consulting) Services the frequency of the transfer is determined by the relevant Transaction Document.   |

|  |  |
|--|--|
| <b>B5</b>  | Nature of the processing: shall be completed with the information set out in Schedule 1, section 6.  |
| <b>B6</b>  | Purpose of the data transfer and further processing: <ul style="list-style-type: none"> <li>(i) for <b>Module Two</b> (controller to processor) SCCs: the purpose of the data transfers and processing is to enable data importer to provide the data exporter with information security services (as set out in the applicable Transaction Document, service level agreement, Service descriptions or otherwise);</li> <li>(ii) for <b>Module One</b> (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, (c) research and analytics, and (d) provision of customer support.</li> </ul> |
| <b>B7</b>  | Period of time for which personal data will be retained: shall be completed with the information set out in Schedule 1, section 7.   |
| <b>B8</b>  | 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.  |
| <b>Annex I.C</b>   |  |
| 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 CRA).  |  |
| <b>Annex II (Security measures)</b>  |  |
| 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 Schedule 2 (Security Measures) of the DPA. |  |

## 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**") issued by the UK Information Commissioner shall apply and shall be incorporated by reference into, and form part of, this DPA, and will come into effect, where applicable, upon signature by the parties of the DPA. Capitalised terms used in this section 2 that are not defined in the DPA shall have the meaning set out in the Addendum.

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

| <b>Table 1: Parties</b> |   |
|-------------------------|---|
| <b>Start date</b>       | This Addendum will start: <ul style="list-style-type: none"> <li>(i) if the Customer has signed an offline CRA, on the same date as such CRA is executed; or</li> </ul> |

|   |  |   |
|---|--|---|
|   | (ii) if the Customer is trading under the online CRA, on the date of execution of the relevant Transaction Document  |   |
| The Parties   | Exporter (who sends the Restricted Transfer):  | Importer (who receives the Restricted Transfer):                                |
|   | The data exporter (as defined in Schedule 3, section 1.2)  | Secureworks Inc. (as specified in Schedule 3, section 1.2)                      |
| Parties' details and key contacts   | As set out in Schedule 3, section 1.2 or otherwise notified between the parties  |   |
| Signature   | The Addendum shall be deemed to have been signed by the parties as set out in Schedule 3, section 1.2.   |   |
| 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"><li>– Clause 7 (Docking clause): the docking clause shall apply</li><li>– Clause 11 (Redress): the optional wording in Clause 11(a) shall <b>not</b> apply</li></ul>   |   |
| Module Two:   | <ul style="list-style-type: none"><li>– Clause 7 (Docking clause): the docking clause shall apply</li><li>– Clause 11 (Redress): the optional wording in Clause 11(a) shall <b>not</b> apply</li><li>– Clause 9(a) (Sub-processors): <b>Option 2: General written authorisation</b> is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) days in advance</li></ul> |   |
| Table 3: Appendix Information   |  |   |
| “ <b>Appendix Information</b> ” 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 this Addendum is set out as follows: |  |   |
| Annex I.A: List of Parties:   |  | See Schedule 3, section 1.2   |
| Annex I.B: Description of Transfer:   |  | See Schedule 3, section 1.2   |
| Annex II: Technical and organisational measures   |  | See Schedule 2  |
| Annex III: List of Sub processors:  |  | See Clause 4.6 of the DPA   |
| Table 4: Ending this Addendum when the Approved Addendum changes  |  |   |
| Ending this Addendum when the Approved Addendum changes   |  | Which Parties may end this 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 Two (controller 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 Two (controller to processor) SCCs: |   |
|---|---|
| <b>Clause 7 (Docking clause)</b>  | The optional docking clause shall apply.  |
| <b>Clause 11(a) (Redress)</b>   | The optional wording in Clause 11(a) shall <b>not</b> apply.  |
| <b>Clause 13 (Supervision) and Annex I.C</b>  | <ul style="list-style-type: none"> <li>– Where the transfer is exclusively subject to Swiss Data Protection Laws: FDPIC.</li> <li>– Where the transfer is subject to both Swiss Data Protection Laws and GDPR:</li> </ul> |



|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>(i) FDPIC is the supervisory authority insofar as the transfer is governed by Swiss Data Protection Laws; and</li> <li>(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).</li> </ul>   |
| <b>Clause 17<br/>(Governing law)</b>                                       | <ul style="list-style-type: none"> <li>– Where the transfer is exclusively subject to Swiss Data Protection Laws: Swiss law is the governing law.</li> <li>– 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.</li> </ul> |
| <b>Clause 18(b)<br/>(Choice of forum and jurisdiction)</b>                 | <ul style="list-style-type: none"> <li>– Clause 18(b): The courts of the country in which the data exporter is established</li> <li>– 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.</li> </ul>   |
| <b>Annex I.A</b>   | For a list of the parties see Schedule 3, section 1.2.   |
| <b>Annex I.B</b>   | For a description of the transfer see Schedule 3, section 1.2.   |
| <b>Annex II</b>  | For the technical and organisational measures see Schedule 2.  |
| <b>Swiss amendments to ONLY Module Two (controller to processor) SCCs:</b> |  |
| <b>Clause 9(a)<br/>(Use of sub-processors)</b>                             | <b>Option 2: General written authorisation</b> is selected. Data importer shall inform the data exporter of any intended changes to its list of sub-processors at least fourteen (14) days in advance.   |
| <b>Annex III (List of sub-processors)</b>                                  | See Clause 4.6 of the DPA.   |

3.5 **Supplemental** – The SCCs shall protect the data of legal entities in Switzerland until the entry into force of the Revised FADP (effective 1 January 2023).

3.6 **Incorporation** – The SCCs (Module One and Module Two) adapted for Switzerland in accordance with this section 3 shall apply and shall be incorporated by reference into, and form part of, this DPA and will come into effect, where applicable, upon signature by the parties in accordance with Schedule 3, section 1.2.

**SCHEDULE 4 TO DATA PROTECTION ADDENDUM**  
**Compliance with GERMAN and SWISS criminal law**

**1. Scope**

(i) This Appendix applies to all Services provided in or accessed from Germany and are intended to avoid any possible criminal liability in Germany (German cyber security law, esp. sec. 202a et seq, 203, 206, 303a, 303b German Criminal Act [StGB]).

(ii) This Appendix also applies to all Services provided in or accessed from Switzerland and are intended to avoid any possible criminal liability in Switzerland (Swiss cyber security law, esp. articles 143, 143bis, 144bis, 147, 150, 179 et seq Swiss Criminal Code [StGB]).

Customer acknowledges its acceptance with the German or the Swiss criminal law provisions set out herein if the Services are provided in or accessed from Germany or Switzerland, as the case may be.

**2. Security Services, further security measures and other Services as performed by Secureworks**

2.1 Should a Transaction Document include security scanning, testing, assessment, forensics, or remediation Services ("**Security Services**"), Secureworks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. The Security Services, such as penetration testing or vulnerability assessments, may entail buffer overflows, fat pings, operating system specific exploits and attacks specific to custom coded applications but will exclude intentional and deliberate Denial of Service ("DoS")-Attacks. Secureworks shall perform Security Services during a timeframe mutually agreed upon with Customer.

2.2 The aforementioned Security Services as well as all further security measures to be performed under the CRA, the Transaction Documents as well as other Services to be taken by Secureworks hereunder may result in:

- (a) Secureworks obtaining personal and other private data of individuals and/or third parties (e.g. customers of Customer, Customer employees) located on Customer's IT-systems concerned by the performance of Services hereunder, in particular by:
  - (i) the circumvention of Customer's security systems which are especially protected against unauthorized access; and/or
  - (ii) the interception of data by technical means from a non-public data processing facility (e.g. e-mail communication).
- (b) Secureworks directly or, if applicable, as a result of performing the Services, deleting, suppressing, rendering, making unusable or altering data and/or interfering with data processing operations by destroying, damaging, rendering making unusable, removing or altering a data processing system or a data carrier and/or
- (c) service interruptions or degradation regarding the Customer's systems.

2.3 Secureworks will treat any data which may be subject to the postal or telecommunications secret and/or further contractual and/or statutory business secret (e.g. data subject to Section 203 German Criminal Code [StGB]) as confidential. Secureworks will only obtain knowledge of the content or the specific circumstances of the data obtained to the extent necessary for the protection of the Customer's IT-systems.

3. **Customer consent with respect to intrusion attempts and Customer's system security checks**

- 3.1 Customer authorizes Secureworks to perform the Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services) on network resources with the internet protocol addresses ("**IP Addresses**") identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party, in the necessary form and substance satisfactory to Secureworks, to permit Secureworks to provide the Security Services on such third party's network resources.
- 3.2 In light of the foregoing, upon execution of a Transaction Document for the aforementioned Security Services, Customer consents and authorizes Secureworks to provide any or all the Security Services in the applicable Transaction Document with respect to the Customer's systems. Customer further acknowledges it is the Customer's responsibility to restore network computer systems to a secure configuration after completion of Secureworks's testing. Customer acknowledges and accepts the risks and consequences as laid out above under 2.2.
- 3.3 The Customer acknowledges and explicitly declares its consent that Secureworks may in this context involve Secureworks' subcontractors and/or other Secureworks Affiliates located around the world (e.g. Secureworks Inc. in the United States, Secureworks Europe SRL in Romania, Secureworks entities located in Asian countries) in order to provide the Services to be performed under the CRA and the Transaction Documents, including the security measures described above. Secureworks undertakes to require any Secureworks subcontractor and/or any other Secureworks Affiliate that Secureworks may involve in order to provide the aforesaid services to treat any data which may be subject to the postal or telecommunications secret and/or further contractual and/or statutory business secret (e.g. data subject to Section 203 German Criminal Code [StGB] or data subject to Article 321 Swiss Criminal Code [StGB]) as confidential.

4. **Customer guarantee to provide necessary consents**

- 4.1 Customer hereby guarantees with respect to the provision of Services by Secureworks:
- (a) that it has obtained all necessary consents, authorization and required permissions in a valid manner to enable Secureworks to conduct all system security checks and provide to Secureworks respective proof upon Secureworks's request;
  - (b) that by implementing all necessary technical and organizational measures it will safeguard that Secureworks will only be enabled to conduct or be requested to conduct system security checks on the network resources to the extent as agreed upon by the Parties.
- 4.2 Customer shall document the obtaining of all necessary consents, authorization and required permissions audit-proof, and shall, upon Secureworks' request and at Secureworks' discretion, provide Secureworks with the documentation in order to enable Secureworks to prove compliance.