Standard Contractual Clauses (C-to P Transfers) for McAfee Suppliers

Unless Supplier informs McAfee and requires specific modifications to the below, the following the Standard Contractual Clauses, including its exhibits, will be deemed executed between the parties.

Unless you (hereinafter the "**Supplier**") have entered into a valid agreement with McAfee, this Data Processing Exhibit ("**Data Processing Exhibit**") is governed by and subject to the terms and conditions available at https://www.mcafee.com/enterprise/en-gb/about/legal/contracts-terms.html (the "**Agreement**").

1. DEFINITIONS

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. DETAILS OF THE TRANSFER

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 of Schedule 1 which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6.1 and 6.2, Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have

become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4.   **OBLIGATIONS OF THE DATA EXPORTER**

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 of Schedule 1;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

5.   **OBLIGATIONS OF THE DATA IMPORTER**

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 of Schedule 1 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

(i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii)   any accidental or unauthorised access, and

(iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 of Schedule 1 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6.   LIABILITY

6.1   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2   If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7.   MEDIATION AND JURISDICTION

7.1   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8.   COOPERATION WITH SUPERVISORY AUTHORITIES

8.1   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9.   GOVERNING LAW

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10.   VARIATION OF THE CONTRACT

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11.   SUB-PROCESSING

11.1   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2   The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent

and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3   The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the data exporter is established.

11.4   The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

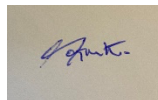12.   OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

12.1   The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2   The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 12.1.

On behalf of the data exporter:

Name (written out in full):   Roy Kamp

Position: Data Protection Officer

Address: McAfee, LLC on behalf of McAfee Ireland and all its Affiliates

                                               6220 America Center Drive San Jose, CA 95002. USA

Signature:

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Signature:

Schedule 1

Appendices to the Standard Contractual Clauses: C-to-P Transfer

---

APPENDIX 1 OF SCHEDULE 1 - DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

This Appendix forms part of the Transfer Clauses and must be completed and signed by the Parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The Data Exporter is McAfee Ireland Limited on behalf of McAfee, LLC and its Affiliates worldwide, a global provider of security products and services.

Data importer

The Data Importer is the Supplier on behalf of itself and its Affiliates worldwide ("Data Importer"). The Data Importer provides products and/or services to the Data Exporter in relation to the Agreement, in the course of which it processes certain personal data as a processor.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

      ☒ Current, former, prospective employees.

      ☒ Current, former, prospective employees and their dependents.

      ☒ where applicable Employees of Corporate customers

      ☒ where applicable McAfee consumer customers and former consumer customers

      ☒ Customer contacts

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify):

      ☒ Employees' names and contact information, including addresses, emails, phone numbers, IP addresses, employment history, education/qualifications, transaction history.

      ☒ Employees' names and contact information, including addresses, emails, phone numbers, IP addresses; employees' dependents' names and contact information, including addresses, emails, phone numbers, transaction history.

      ☒ McAfee Corporate customers' employees' names and business contact information, including addresses, emails, phone numbers, IP addresses, transaction history, payment information.

      ☒ McAfee Consumer customers' names and business contact information, including addresses, emails, phone numbers, IP addresses, transaction history, payment information.

      ☒ Customer contacts, including employees' names and business contact information, including addresses, emails, phone numbers, IP addresses, transaction history, payment information.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

☒ None.

☐ If you are using / transferring any information about children or an individual's racial/ethnic origin; health; sexuality; political opinions; religious beliefs; criminal background or alleged offences; or trade union membership, this should be noted here:

Please elaborate:

Processing operations

The personal data transferred will be subject to the following basic processing activities (please untick any non-applicable purpose):

☒ The Personal Data will be used to provide for providing any and all products and services contemplated under the Agreement.

This Appendix 2 forms part of the Transfer Clauses and summarizes the technical, organisational and physical security measures implemented by the parties in accordance with Clauses 4(d) and 5(c).

In addition to any data security requirements set forth in the Agreement as amended by the Data Privacy Exhibit, Supplier shall comply with the following, unless otherwise indicated below and approved by McAfee.

1. Introduction

These Supplier Security and Privacy Requirements ("SSPRs") establish Supplier's minimum-security standards for protection of McAfee Confidential Information, including McAfee Personal Data.

To achieve security compliance, Suppliers and their subcontractors are wholly responsible for implementing all the security controls defined herein to protect the data they manage, host or process for any function or activity implemented on behalf of McAfee. This SSRE is not intended to be an all-inclusive list of security requirements. Each solution may generate unique or specific requirements that must be addressed with the appropriate security controls and defined in the applicable statement of work executed by the parties. This SSRE should be reviewed by the Supplier's Chief Information Officer (CIO) or Security Officer responsible for contracted services. It is the responsibility of the primary Supplier to review the SSRE with its subsidiaries and subcontractors responsible for service delivery to McAfee or on behalf of McAfee and to ensure subcontractor's compliance herewith. The Supplier is responsible for conformance to the SSRE when services are performed by itself, its subsidiaries or its subcontractors. This version of the SSRE covers data classified up to Confidential. The McAfee business owner is responsible for classifying the data of their web application and communicating it to the Supplier. At a minimum, Suppliers must be capable of implementing security controls required to protect data classified as Confidential.

Supplier must ensure their subsidiaries and subcontractors are compliant with all regulatory and local governing laws as well as Data Protection Laws for the services under contract to McAfee. Examples include, but are not limited to, GDPR, CCPA and CAN-SPAN Act compliance. Suppliers are responsible for compliance with any laws and regulatory requirements applicable to their use of the system.

2. General undertakings

Suppliers shall review all security controls cited in this document and may request clarification where needed. Suppliers shall notify the appropriate McAfee business owner of full compliance in writing authorized by a company official. Existing Suppliers that complied with a previous version of the SSRE must review and adhere to instructions in this document as McAfee may have included important updates/changes from previous versions. If a Supplier, their subsidiaries, or subcontractors are not fully compliant to all minimum-security requirements, the Supplier shall provide in writing the extent of non-compliance and give committed plan of action detailing when the requirements will be fully met. McAfee's Information Security team shall evaluate a Supplier's security capability. If approved by McAfee, the Supplier plans will be documented in the contract. During a contract review, a Supplier's performance of the SSRE security requirements, the completion of non-compliant security controls plus the Supplier's track record for prompt remediation of vulnerabilities will be evaluated.

Suppliers shall agree to fully comply with the McAfee Code of Conduct, as set forth at McAfee's Supplier Ethics Expectations portal and the Electronic Industries Code of Conduct as set forth at http://www.eiccoalition.org/standards/code-of-conduct/. Additionally, while performing services in McAfee owned or operated facilities, Suppliers shall agree to abide by all McAfee Corporate and Security Policies while performing such services including, but not limited to, safety, health and hazardous material management rules, and rules prohibiting misconduct on Buyer's premises including, but not limited to, use of physical aggression against persons or property, harassment, and theft. Suppliers will perform only those services identified in a duly executed statement of work and will work only in areas designated for such services. Suppliers shall take all reasonable precautions to ensure safe working procedures and conditions for performance on McAfee premises and shall keep McAfee's site neat and free from debris.

Supplier agrees to implement data protection by design and by default and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier implements the following measures:

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effective of technical and organizational measures for ensuring the security of the processing.

Supplier acknowledges that Personal Data retention and replication should always be assessed against business need and minimised, either by not collecting unnecessary data or by deleting data as soon as the need for it has passed and that holding any Personal Data presents security risks.

3.   Cloud Services and Systems

Cloud-based systems may only contain McAfee Confidential Information subject to the prior written approval of McAfee and must be certified to ISO 27001 standards as a minimum. McAfee reserves the right to perform a security review and risk assessment of applications and services containing McAfee Confidential Information in the cloud prior to implementation. Any changes to the architecture or function of a service or data model in the cloud that stores McAfee Confidential Information must first be reviewed and approved by McAfee Information Security Department. Applications that require physical separation cannot be on a cloud-based service unless duly segregated and approved in writing by McAfee. Supplier shall ensure McAfee Confidential Information is fully segregated from Supplier's other customers and/or third parties. In addition, Supplier agrees to allow any regulated End-User Customers(i.e. when a government or regulatory body with binding authority ("Regulator") regulates such entity's regulated services such as (for example) financial services) or any independent or impartial inspection agents or auditors selected by McAfee or a regulated End-User Customer, to audit Supplier and Supplier agrees to allow McAfee to provide any such reports to its End-User Customers where required.

4.   Vulnerability Management

If Supplier is hosting a public-facing McAfee website, Supplier shall perform daily vulnerability scans on all internet facing web sites where McAfee has branded content, McAfee is the primary site owner or 'McAfee' is part of the URL. McAfee uses the McAfee Secure vulnerability scanning solution. Vulnerabilities will be reported to the Supplier for remediation. Supplier can request information for vulnerability reports, demonstration of the vulnerabilities (when available) and remediation support. McAfee will not charge Supplier for the McAfee Secure scanning service. McAfee requires daily access to the reports. Upon identification of security vulnerabilities in a production application, Supplier must remediate within the minimal following time lines: (i) Urgent or Critical, McAfee threat rating [5] or [4] must be remediated in 1 to 5 calendar days; (ii) High, McAfee threat rating [3] must be remediated within 10 calendar days and (iii) Medium, McAfee threat rating [2] must be remediated within 30 calendar days.

If the security vulnerabilities identified by the McAfee vulnerability scanning process have not been addressed in the above timelines, McAfee may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for McAfee compliance. McAfee considers a web site compliant when McAfee security standards are met. McAfee will notify Suppliers any time the McAfee security standards not met.

5.   Organizational Measures

The implementation and operational effectiveness of all below controls are mandatory. The below organizational measures are derived from McAfee's Third-Party Information Security Risk requirements, which align to leading industry standards. ***Unless Supplier informs McAfee and requires specific modifications to the below, the following Organizational Measures will be deemed agreed upon by the Supplier***.

Organizational Measures			
- Supplier has a specific resource assigned that is accountable for security management. - All systems have malware management which includes up to date signature files running on all production systems. - If administration of any systems or applications is performed outside the Suppliers secured intranet, it must be done through a secure channel (VPN or SSL)			
Control Title	**Control Description**	**Reference to Industry Standard**	**Implemented? (Yes/No)**
Governance Personnel	Supplier has appointed designated governance staff on the topic of Information Security and Data Privacy to ensure compliance with industry requirements (E.g. Data Protection Officer, Information Security Officer)	ISO 27701 6.3.1.1	Yes
Industry Standards	Supplier follows industry standards and laws, regulations, and applicable guidelines. Supplier is certified against (at a minimum) the ISO 27001 standard and has a periodic cycle of internal and external audits to ensure the continued compliance of all applicable security controls. Supplier shall submit a copy of any industry standard accreditation applicable to the products or services it is providing to McAfee (e.g., ISO27001, PCI-DSS or	ISO 27001 A.12.7.1	Yes

	SSAE16/18-SOC 2 audits performed by an independent auditor within the last year) and provide annual updates of the accreditation during the term of the Agreement. Supplier shall also inform McAfee of its adherence to data protection certification.		
Privacy & Protection of Personal Data	Supplier takes measures to ensure protection of Personal Data as required with relevant legislation such as the GDPR. At a minimum, Supplier encrypts data at rest and in transit as required by law, regulation, and applicable guidelines.	ISO 27001 A.18.1.4	Yes
Information Security Policies	Information security policies are implemented within the Supplier and available to all employees. Such policies are reviewed at planned intervals by appropriate personnel to ensure their continued effectives to the organization	ISO 27001 A.5.1.1 ISO 27001 A.5.1.2	Yes
Segregation of Duties	Conflicting duties shall not be granted to an employee, Eg roles/permissions in an IT application. In addition, IT environments should be segregated where appropriate (development vs test environment etc.)	ISO 27001 A.6.1.2 ISO 27001 A.12.1.4	Yes

Information Security & Privacy Awareness

- Supplier personnel must be trained in Supplier security policies and be required to know changes or updates to these policies.
- Security training, including new threats and vulnerabilities, is required for all developers and system administration staff.
- All personnel with access to confidential data will have information security training for their respective roles.
- All personnel receive regular updates to their training for their respective roles.
- All personnel with access to Personal Data will complete a privacy training class and be knowledgeable and of any specific privacy requirements for the data being handled. This training will be provided by the Supplier or by accessing https://www.mcafee.com/us/about/legal/privacy.aspx. Refresh training is required annually.
- All development staff should be trained on secure coding principles and best practices. Training materials are updated on an ongoing basis to include new threats and vulnerabilities.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Employee Screening	Supplier has appointed designated governance staff on the topic of Information Security and Data Privacy to ensure compliance with industry requirements (E.g. Data Protection Officer, Information Security Officer)	ISO 27001 A.7.1.1	Yes
Contractual Obligations	Contracts with both employees and contractors shall state employee obligations for information security and data privacy both during and after termination of employment	ISO 27001 A.7.1.2 ISO 27001 A.7.3.1	Yes
Information Security & Privacy Training	All employees shall receive appropriate education on the topics of information security and data privacy, and remain informed on updates to organizational policies such as the Information Security Policy	ISO 27001 A.7.2.2	Yes

IT Asset Management

- All data provided by McAfee shall be considered Confidential.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Asset Register	A dedicated IT asset register is operational and is maintained which identifies key information at asset-level such as owner	ISO 27001 A.8.1.1 ISO 27001 A.8.1.2	Yes

Acceptable Use	Formalized policy exists and is available to all employees on the topic of acceptable use of IT assets such as company laptops/desktops	ISO 27001 A.8.1.3	Yes
Return of IT Assets	Upon termination of employment, end users return all company-owned IT assets	ISO 27001 A.8.1.4	Yes
Information Classification	All data provided to the Supplier shall be considered Confidential. Such rules should be adopted organization-wide in a dedicated policy/procedure document, and should be considered when handling information as part of operational activities	ISO 27001 A.8.2.1 ISO 27001 A.8.2.2 ISO 27001 A.8.2.3	Yes
Removable Media Devices	Sensitive information on media leaving the Supplier's premises should be protected to ensure access is restricted to the appropriate personnel (E.g. by means of encryption)	ISO 27018 A.11.4	Yes
Management & Destruction of Media	Formalized procedures shall be implemented to ensure lifecycle management of removable media in accordance with Information Security Policies	ISO 27001 A.8.3.1 ISO 27001 A.8.3.2 ISO 27001 A.8.3.3	Yes

User Access Management

Supplier has a duty to limit access to personal data on a "need to know" basis. Supplier is required to assess the nature of access allowed to an individual user. Supplier agrees that individual staff members shall only have access to data which they require in order to perform their duties, prevent use of shared credentials (multiple individuals using a single username and password) and detect use of default passwords. Access control must be supported by regular reviews to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a function. Supplier has policies in place in regard to vetting and oversight of the staff members allocated these accounts. A staff member with similar responsibilities should have separate user and administrator accounts. Multiple independent levels of authentication may be appropriate where administrators have advanced or extra access to personal data or where they have access or control of other's account or security data. Supplier agrees to have strict controls on the ability to download personal data from an organisation's systems. Supplier agrees to block such downloading by technical means (disabling drives, isolating network areas or segments, etc.).

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
User registration and de-registration	A formal process should exist to management the assignment, adjustment, and revoking of access rights, considering scenarios such as starters/leavers as well as changing of jobs internally within the organization	ISO 27001 A.9.2.1 ISO 27001 A.9.2.2 ISO 27001 A.9.2.6	Yes
Least Privileged Access / Role Based Access	End users shall only be provided with access to IT/network applications based on the requirements of their role within the organization. By default, an end user should have access to a limited amount of IT resources (i.e. email) unless otherwise authorized by appropriate personnel. In circumstances where an end user requires access to a specific IT application, the minimal level of access required to perform their duties should be granted	ISO 27001 A.9.1.2	Yes

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Passwords	Passwords should be implemented on all IT applications and should not be shared. Passwords should be stored in encrypted form. All passwords must meet the following complexity requirements: -Minimum length of 8 characters -Must contain at least 1 upper-case character -Must contain at least 1 number -Must contain at least 1 special character -Must not be the same as the last 24 passwords used -Accounts are locked after 5 incorrect login attempts	ISO 27001 A.9.2.4 ISO 27001 A.9.3.1 ISO 27001 A.9.4.2 ISO 27001 A.9.4.3	Yes
Unique Use of User IDs	End users should each be assigned an individual user ID or identifier for accessing IT resources to ensure accountability. In circumstances where generic user IDs may exist for various business reasons, only one (1) user should have access to such accounts	ISO 27018 A.11.8	Yes
User Access Reviews	End user access to IT applications/resources should be reviewed periodically at defined intervals by appropriate personnel (E.g. application owner, line manager) to ensure all end users within the organization have the appropriate level of access to perform their duties, and that excessive access rights are not granted	ISO 27001 A.9.2.5	Yes

Physical & Environmental Security

In addition to technical security measures, Supplier has implemented the physical security measures which are necessary to ensure the security and integrity of any Personal Data processed. The physical security measures include at minimum:

- perimeter security (monitoring of access, office locked and alarmed when not in use);
- restrictions on access to sensitive areas within the building (such as server rooms);
- computer location (so that the screen may not be viewed by members of the public);
- storage of files (files not stored in public areas with access restricted to staff with a need to access particular files); and
- secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Building Security (Perimeter)	Physical security mechanisms for entering the premises are implemented to ensure that only authorized individuals have access	ISO 27001 A.11.1.1	Yes
Building Security (Internal)	Additional physical security mechanisms for entering areas which contain critical/sensitive information should be restricted to the appropriate personnel (E.g. server room). Video surveillance/intrusion detection capabilities should monitor access to such working area entry points	ISO 27001 A.11.1.2 ISO 27001 A.11.1.3 ISO 27001 A.11.1.5	Yes
User Workspace	Supplier-managed devices such as laptops should have appropriate mechanisms installed to ensure protection when unattended. In support of such, a clean desk policy shall be implemented to minimize the existence of physically stored information	ISO 27001 A.11.2.8 ISO 27001 A.11.2.9	Yes

Operational Security

- Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
- All data provided by McAfee should be encrypted using AES-128 or stronger.
- To protect data Integrity, data should be hashed using SHA-256 or stronger.

- All Confidential hard copy data that is no longer required must be shredded by use of a crosscut shredder.
- The print process must be adequately secured to prevent unauthorized disclosure/access.
- Extra precautions must be in place to protect the confidential data stored on portable systems or mobile devices. Devices and data must be stored securely when not in use. Portable systems with confidential data must not transfer data by use of Personal Area Networks.
- Web sites and applications must be backed up in accordance with Business Continuity and Disaster Recovery requirements.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Information Backup & Restoration	Backup copies of appropriate information shall be taken as well as tested regularly in accordance with Supplier's backup policy	ISO 27001 A.12.3.1	Yes
Event Logging	Event logging should be enabled in IT applications to record actions such as user activities and reviewed periodically to monitor potential information security events	ISO 27001 A.12.4.1	Yes
Change Management	Changes to business processes or IT applications should be controlled by means of a formalized process, such as a change request process or governed by a change advisory board (CAB)	ISO 27001 A.12.1.2	Yes
Malware Controls	Capabilities to prevent against and to detect malware should be implemented which are applicable to all IT resources (E.g. by means of antivirus software, firewalls etc.). All such solutions should be kept up to date.	ISO 27001 A.12.2.1	Yes
Vulnerability Management	Supplier shall define a process to identify and remediate vulnerabilities to IT applications (E.g. a patch management process)	ISO 27001 A.12.6.1	Yes
End-User Software Installation	Supplier shall define rules to govern the installation of software on company devices by end users. Where possible, software should not be installed on company-managed devices by anyone other than IT administrators	ISO 27001 A.12.6.2	Yes

Communications Security

- Supplier must secure all backup media during transportation and in storage.
- Supplier should catalog all media so that a missing storage unit (and which unit it is) shall be easily identified. Supplier should not label media in such a way that it discloses the data it contains or its owner company in a manner that is easily identified by an outsider.
- Supplier should maintain system and application backups that support a total system restore for a 30-day period as a minimum. Backup media must be on separate media from the system.
- Supplier must destroy all confidential data within 30 days of termination of Supplier contract.
- Copies of Confidential Data on system backup media that is co-mingled with other system data are not included

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Network Security	Corporate network is controlled to protect information by means of security mechanisms and resourcing (incl. segregated where appropriate)	ISO 27001 A.13.1.1 ISO 27001 A.13.1.2 ISO 27001 A.13.1.3	Yes
Encryption of Data	Sensitive information shall be encrypted during transmission	ISO 27001 A.13.2.1	Yes

Incident Management

As part of a data security policy, Supplier has a policy in place describing what it does in case of a data breach, and represents it has the capacity to respond adequately in order to cover the requirements of mandatory breach reporting (where applicable) under applicable Data Protection Laws.

- Any security event involving or impacting McAfee and/or a McAfee website must be reported to McAfee. Notification must be within 48 hours from detection if McAfee data, the McAfee brand, logo or trademarks are involved or compromised.
- Any security event where a McAfee website had unauthorized access or was compromised must be reported to McAfee.
- All systems and applications must be designed to log, monitor and report all security events. Logs must be tampered proof and/or off system write only log files.
- In the event of an incident, audit trails must be available to assist investigations. McAfee may request to cooperatively work with the Supplier on security forensics for some incidents.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
Incident Detection & Response	Supplier has in place a formalized structure (E.g. a security operations center) to ensure detection and response to information security events which may be deemed as an incident	ISO 27001 A.16.1.1 ISO 27001 A.16.1.2 ISO 27001 A.16.1.3 ISO 27001 A.16.1.4 ISO 27001 A.16.1.5	Yes
Employee Reporting	Employees/contractors have mechanisms available to report potential incidents or security weaknesses observed		Yes

Business Continuity & Disaster Recovery (BCDR)

- Cloud-based services require a non-cloud-based solution as one of the Business Continuity / Disaster Recovery options in the event of an incident.
- Supplier must have a disaster recovery plan in place in the event that a major disruptive incident impacts their ability to provide service.
- Mission or business critical functions must have a recovery or continuity plan in place per the mutually agreed upon Service Level Agreement.
- Defined strategies must be tested annually and revised where necessary.
- All system media has a regularly scheduled backup and restore capability implemented and tested.
- Supplier personnel responsible to support business and disaster recovery functions must be identified to McAfee upon request.

Control Title	Control Description	Reference to Industry Standard	Implemented? (Yes/No)
BCDR Processes	Supplier has in place contingency plans or business recovery strategies, which are inclusive of the concepts of Information Security & Privacy	ISO 27001 A.17	Yes

6. Server Security
6.1 Intrusion Detection

- All production servers must be located in a secure, access-controlled location.
- All systems must be hardened prior to production use including patching of known vulnerabilities. Disable all generic, guest, maintenance and default accounts.
- Patching of security vulnerabilities to the operating system and software must meet or exceed the service level interval defined by the vendor for the threat level of the vulnerability.
- Test accounts and user accounts are removed/revoked when no longer required.
- Development and test systems are isolated from production environment and network.
- Disable all non-required ports and/or services on server operating systems and firewalls.
- Consoles with keyboards have password protected screen savers that logoff unattended.

6.2 Virtualized System

- All Intrusion Detection Systems in place should be configured to provide data on demand, to identify sources of a potential attack/intrusion at the network perimeter.
- Systems should have the ability to detect a potential hostile attack. Examples include but are not limited to: Network Intrusion Detection or Host Intrusion Detection/Prevention.
- Any single image of data classified as Confidential defines the minimum-security requirement for all virtual instances on the same host system.
- Virtualized systems may contain data classified as confidential data. (c) Applications that require physical separation cannot be on the same host system.

6.3 Cloud Services and Systems

- Any single image of data classified as Confidential defines the minimum-security requirement for all virtual instances in the cloud.
- Cloud based systems may contain confidential data. McAfee reserves the right to perform a Security review and Risk Assessment of applications and services containing confidential data in the cloud before implementation.
- No services will be run from the cloud that interacts with data exceeding the McAfee classification of "Confidential". (d) Existing services containing confidential data may not be pushed to the cloud or transferred to cloud service vendors without McAfee approval. It is subject to approval following a Security review and Risk Assessment by McAfee.

7. General Requirements

7.1 Application Development

- The application and associated databases must validate all input.
- Implement safeguards against attacks (e.g. sniffing, password cracking, defacing, backdoor exploits)
- Protect the data by using a least privilege and a defense-in-depth layered strategy to compartmentalize the data.
- Handle errors and faults by always failing securely without providing non-essential information during error handling.
- Log data to support general troubleshooting, audit trail investigative requirements, and regulatory requirements, with support for centralized monitoring where appropriate.
- Built-in security controls – built-in access controls, security auditing features, fail-over features, etc.
- Prevent buffer overflows.
- Avoid arithmetic errors.
- Implement an error handling scheme. Error messages should not provide information that could be used to gain unauthorized access.
- Test data used during development must be non-production simulated data.
- Implement protocols (TCP/IP, HTTP, etc.) without deviation from standards.

7.2 Security Reviews:

- Web application vulnerability assessments must be performed during the application development and the deployment lifecycle.
- All 3rd party software included in the application must meet all security requirements outlined herein.
- Secure interfaces for USER LOGIN and user data input of Personal Data must utilize certificates signed by a trusted Certificate Authority (CA) only. Examples: HTTPS / TLS / SSH.

7.3 Security of System Files

- Access to source code must be limited and controlled.
- During and after development, all applications must ensure the security of system files, plus access to source code and test data.
- All back-door maintenance hooks must be removed from the application before production use.
- Application architecture must prohibit databases containing confidential information from residing on the same server as the application.
- Databases must be secured as well as the applications and servers on which they reside. (f) Confidential Data is prohibited from residing on systems that have Peer-to-Peer (P2P) applications or Personal Area Networks (PAN).

7.4 Application Availability

- All applications should be designed to minimize the risk from denial of service attacks.
- All applications should limit resources allocated to any user to the minimum necessary to perform the task.
- All applications must prevent unauthenticated users from accessing data or using vital system resources.

7.5 Vulnerability Management

- Supplier is responsible for running its own vulnerability management.
- In addition, McAfee requires daily vulnerability scans performed on all internet facing web sites where McAfee has branded content and is the primary site owner or 'McAfee' is part of the URL. McAfee uses the McAfee Secure vulnerability scanning solution. Vulnerabilities will be reported to the Supplier for remediation. The Supplier can request information for: vulnerability reports, demonstration of the vulnerabilities (when available) and remediation support. McAfee does not charge the Supplier for the McAfee Secure scanning service.
- McAfee requires daily access to the reports.
- Upon identification of security vulnerabilities in a production application, the Supplier must remediate within the following time lines:

- o Critical: 7 days
- o High: 30 days
- o Medium: 90 days
- o Low: 180 days
- If the security vulnerabilities identified by the McAfee vulnerability scanning process have not been addressed in the above timelines, McAfee may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for McAfee compliance.
- McAfee considers a web site compliant when McAfee security standards are met. McAfee Security will notify Suppliers of each of the McAfee security standards not met.
- Any changes to the architecture or function of a service or data model in the cloud must first be reviewed and approved by McAfee.
- Applications that require physical separation cannot be on a cloud-based service.
- Cloud vendors are required to have background checks and validation of employees with privileged account access. This includes any third-party vendors that may contract with those vendors and have privileged access as well.

8. Network & Client Security
8.1 Remote Access

- There should be no dial-in modems on the network without secondary authentication. (Dial back is not authentication).
- Outbound modems (such as for paging) must have inbound calls disabled.

8.2 Client Security

- Patching of security vulnerabilities to the operating system and software must meet or exceed the service level interval defined by the vendor for the threat level of the vulnerability.
- Clients must have Malware protection with automatic signature updates.
- Systems located in an unsecured area and attached to the Supplier network must not access systems and network segments containing confidential data.
- All client systems that access confidential data, whether in use or not, must be physically secured.
- Client systems which access confidential data from secured locations must have a password protected screen saver or automated logoff after no more than 15 minutes of inactivity of account access. This includes any third-party vendors that may contract with those vendors and have privileged access as well.

9. Firewall Setup
- Network segments connected to the Internet must be protected by a firewall and configured to secure all devices behind it.
- All system security and event logs are reviewed regularly for anomalies, and available to McAfee in the event of an incident.
- Unused ports and protocols must be disabled.
- Firewalls must be configured to prevent address spoofing.
- Only TCP ports should be used for web applications.
- Supplier firewalls must be configured to allow McAfee scanning of McAfee Web applications. McAfee scanning source IP addresses will be provided to Suppliers.

10. Data Security
10.1 Data Classification and Handling

- Appropriate security measures must be in place to address data handling, access requirements, data storage and communications (in transit).
- All McAfee data is Confidential.

10.2 Privacy Management

- Applications such as "Software as a Service' used by McAfee to collect Personal Data must have the URL for the McAfee Privacy Statement embedded into the web page where Personal Data is collected. It is available in all languages.
- Where applicable, individuals must be given the opt-in choice to participate prior to providing their Personal Data. Opt-in selection boxes are not pre-selected by default.
- Where applicable, the system should have the capability of allowing individuals to access update or delete their Personally Identifiable Information or unsubscribe when requested. This can be an automated or manual process. The process must be clearly explained to the individual.
- System must not transfer Personal Data to other systems or be used for purposes other than specified.
- System must have appropriate security controls to avoid unauthorized access, disclosure and / or use or modification of individuals' Personal Data.
- The system must adhere to the Federal Trade Commission's CAN-SPAM Act if it:
    - Requests input of Personal Data from an individual to complete "Email to a Friend" notifications, or

- The system offers online, subscription-based communication services.

10.3 Data Protection Security

- Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
1. For data classified as McAfee Confidential, McAfee Confidential – Internal Use Only or McAfee Restricted, data should be encrypted using AES-128 or stronger.
- To protect data Integrity, data should be hashed using SHA-256 or stronger.
- All Confidential hard copy data that is no longer required must be shredded by use of a crosscut shredder.
- The print process must be adequately secured to prevent unauthorized disclosure/access.
- Extra precautions must be in place to protect the confidential data stored on portable systems or mobile devices. Devices and data must be stored securely when not in use.
- Portable systems with confidential data must not transfer data by use of Personal Area Networks
- Web sites and applications must be backed up in accordance with Business Continuity and Disaster Recovery requirements.
- Supplier must secure all backup media during transportation and in storage.
- Supplier should catalog all media so that a missing storage unit (and which unit it is) shall be easily identified. Supplier should not label media in such a way that it discloses the data it contains or its owner company in a manner that is easily identified by an outsider.
- Supplier should maintain system and application backups that support a total system restore for a 30-day period as a minimum. Backup media must be on separate media from the system.
- Supplier must destroy all confidential data within 30 days of termination of Supplier contract. Copies of Confidential Data on system backup media that is co-mingled with other system data are not included.

11. Extranet Requirements

- All extranet connectivity into McAfee must be through secure communications.
- All data exchanged with McAfee for mission or business critical functions, (B2B), require secure intercompany communications (ICC) implemented by McAfee IT Engineering services. The McAfee program manager is responsible for communications funding and will arrange for Suppliers to engage with the McAfee engineering services team.
- Supplier is responsible for implementing the secure protocols at their sites

12. Deviation from Use
Any deviation from the requirements of this standard must be approved in writing by McAfee Information Security.

13. Duration
This standard will remain in effect until cancelled or modified by the McAfee Chief Information Security Officer.

14. Definitions and Abbreviations
Capitalized terms not defined herein shall have the meaning ascribed to such terms in the Agreement.

Application Security: Refers to protecting data processed by an application, as well as the integrity and availability of services provided by the application.

Business Critical: Loss that indirectly impacts a Mission Critical function, or directly impacts a business unit's primary function is considered Business Critical.

Cloud Computing: Computing resources, software and data delivered as a hosted service over the Internet. The computing resources are dynamically scalable and often virtualized. The services are accessible anywhere that provides access to networking infrastructure.

California Consumer Privacy Act of 2018 or "**CCPA**" means Cal. Civ. Code § 1798.100, *et seq.*, as amended

Confidential Data: Information with restricted access limited to those individuals with a need to know.

Content Moderation: A business process where content is reviewed and approved by McAfee or a McAfee representative with the appropriate training before it is viewable by others.

Content Monitoring: A business process where content is reviewed (and removed if necessary) by McAfee or a McAfee representative with the appropriate training after it is viewable by others.

Data Protection Laws means EU Data Protection Laws, the CCPA, and, to the extent applicable, the data protection or privacy laws of any other country.

EU Data Protection Laws means the GDPR and any local data protection laws applicable in the EEA.

EEA means the European Economic Area and Switzerland.

External Facing (Public): Information available without approval or authentication.

GDPR means the European Union (EU) General Data Protection Regulation 2016/679.

Information Security Incident" means any occurrence involving the compromise of McAfee Confidential Information through the accidental or unlawful destruction or loss of McAfee Confidential Information or the unauthorized collection, use, copying, modification, disposal, disclosure, or access of McAfee Confidential Information including Personal Data.

Mission Critical: Loss that directly impacts McAfee's ability to Book, Build, Ship, Order, Pay, Close or Communicate is considered Mission Critical.

Moderation: A business process where McAfee personnel or a contracted agent reviews and either approves or rejects user generated content (UGC) based on the business situation. Automated moderation is when computerized searches are performed on UGC to screen the input for unwanted or malicious input. Community moderation for appropriateness of content is reporting by the user community of violations of content after it is posted.

Physical Security: Measures taken to protect systems, buildings and related support infrastructure against threats from the physical environment.

Personal Data shall have the same meaning as in the Data Protection Laws.

Privacy: An individual's right to have a private life, to be left alone and to be able to decide when their personal information is collected, used or disclosed.

User Generated Content (UGC): Content input into a web application either by text input or rich media such as pictures, audio and videos via file uploads or widgets.

Unsecured Area: Areas that are not controlled by physical access security measures. Some examples are: the lobby of an access controlled building or a warehouse delivery dock with PC access to corporate systems.

Virtualized System: The use of the term 'virtualized system' includes any of the following: A virtual machine (VM) is a software implementation of a computer that executes programs like a real machine. The virtual machine monitor (VMM) or hypervisor is the software layer providing the virtualization. Platform virtualization and /or hardware virtual machines that allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system.

AUTHORIZED THIRD PARTY SUB-PROCESSORS

Please complete the below by inserting name, address and services provided by 3rd party Sub-processors and Affiliates. If this Appendix remains unfilled, Supplier is deemed not to be using any Subprocessor.

Name of Sub-processor	Personal Data being processed	Full address/ Location of processing	Processing activities

SCHEDULE 2 – ANNEX A TO ARGENTINE MODEL CLAUSES

Titulares de los datos	Data owners
Los datos personales transferidos se refieren a las siguientes categorías de titulares de los datos:	The personal data transferred concern the following categories of data owners:
	Refer to Appendix 1, Schedule 1
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
	Refer to Appendix 1, Schedule 1
Características de los datos	Characteristics of the data
Los datos personales transferidos se refieren a las siguientes categorías de datos:	The personal data transferred concern the following categories of data:
	Refer to Appendix 1, Schedule 1
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
Tratamientos previstos y finalidad	*Refer to Appendix 1, Schedule 1*
	Purpose of the data processing to be conducted:
Los datos personales transferidos serán sometidos a los siguientes tratamientos y finalidades:	The transferred personal data will be subject to the following processing and purposes:
	Please refer to the attached "Description of Transfer" document(s)
Consulte *La descripción de la transferencia* adjunta.	*Refer to Appendix 1, Schedule 1*

Data Importer

By:

Name:

Name of the Company:

Title

Address and Country of Company: