McAfee Enterprise Supplier

Data Processing and Security Agreement (DPSA)

This data processing and security agreement ("DPSA") is made between McAfee Enterprise (defined herein) and _____ a _____[*state where incorporated*] company with offices at _____ ("_____" or "Supplier"). McAfee Enterprise and Supplier are collectively referred to as the "Parties."

In consideration of the mutual promises and covenants contained herein and of other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties agree as follows:

This DPSA shall apply to Supplier's provisioning of services to McAfee Enterprise , as set forth in a separate services agreement executed by the Parties, dated _____ (the "Services Agreement").

Scope. This Agreement consists of this front page and the following terms:

Definitions

General Terms

Schedule 1

- **APPENDIX 1 OF SCHEDULE 1 - DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)**
- **APPENDIX 2 OF SCHEDULE 1 TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**
- **APPENDIX 3**

SCHEDULE 2

AS AGREED UPON BY each Party, through its authorized representative:

On Behalf of the Data Exporter: **[Add name of correct legal entity here]**	**On Behalf of the Data Importer:** *[Add Supplier's Full Name]*
Business Address:	Business Address:
Signature:	Signature:
Print Name:	Print Name
Title:	Title:
Date:	Date:

Definitions

All capitalized term shall have the meaning ascribed to them as set forth below.

"**Personal Data**", "**special categories of data**", "**process/processing**", "**Controller**", "**Processor**", "**Data Subject**" and "**supervisory authority**" shall have the same meaning as in the Applicable Law.

"**Adequacy Decision**" means a decision issued under Article 45 of the GDPR.

"**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.

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

"**Argentine Model Clauses**" means the Model Agreement of International Transfer of Personal Data for the case of Provision of Services (*Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios*) (reference: EX-2016-00311578- -APN-DNPDP#MJ- Anexo II) approved by the *Dirección Nacional de Protección de Datos Personales* on 2 November 2016.

"**BCRs**" means the **Binding Corporate Rules** approved in accordance with Article 47 and 63 of the GDPR, which McAfee represents to be in the process of setting in place and which, once approved, will maintain throughout the term of the Agreement, or to the extent made available by the Supplier, which Supplier represents, warrants, and covenants maintaining during the full term of the Agreement.

"Business Critical" means loss that indirectly impacts a Mission Critical function, or directly impacts a business unit's primary function is considered Business Critical.

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

"Confidential Data" means information with restricted access limited to those individuals with a need to know.

"Content Moderation" means 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" means 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, US Federal and State laws, including but not limited to the CCPA, and, to the extent applicable, the data protection or privacy laws of any other country.

"**Data Subject**" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA.

"EEA" means the European Economic Area and Switzerland.

"**End-User Customers**" means McAfee's customers using McAfee products and services and McAfee's partners designated for the reselling and distribution of McAfee products and services.

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

"External Facing (Public)" means 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.

MCCs" means the ASEAN Model Contractual Clauses approved on 22 January 2021 by the Digital Ministers of the Association of Southeast Asians Nations (ASEAN).

"Mission Critical" means a loss that directly impacts McAfee's ability to Book, Build, Ship, Order, Pay, Close or Communicate is considered Mission Critical.

"McAfee Enterprise" means [add here the applicable legal entity name/address]

"Moderation" means 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" means 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.

"**Regulator**" means either (as applicable): (i) an independent public authority which is established by an EU Member State pursuant to Article 51 of the GDPR; or (ii) the California Attorney General.

"**SCCs**" means the EU Standard Contractual Clauses pursuant to European Commission Decision of 4 June 2021, and its Module 2 "Controller to Processor" incorporated herein by reference together with its Appendices attached hereto as Schedule 1.

"**Subprocessor**" means any processor engaged by the Supplier or by any other subprocessor of the Supplier, which agrees to receive from the Supplier, or from any other subprocessor of the Supplier, McAfee or End-User Customers' Personal Data exclusively with the intention for processing activities to be carried out on behalf of McAfee and in accordance with its instructions, the terms of the Agreement, this DPSA and the terms of the written subcontract.

"**Transfer**" means the transfer or disclosure or any other type of access to Personal Data to a person, organisation or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

"**Transfer Mechanism(s)**" means the BCRs, the SCCs, the MCCs, the Argentine Model Clauses and any other transfer mechanism required to undertake a Transfer under Data Protection Laws.

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" means 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" means 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.

-General Terms follow this page-

GENERAL TERMS

1. DETAILS OF THE PROCESSING ACTIVITIES

McAfee Enterprise shall be the Controller or the Processor for its own End-User Customers under the GDPR and "business" under the CCPA (or similar concept under other Applicable Laws) and Supplier and supplier's sub-processors under the GDPR and "service provider" as defined in CCPA section 1798.140 (v) (or similar concept under other Applicable Laws) shall be the Processor regarding the Personal Data processed by Supplier on McAfee's behalf or sub-processed on behalf of End-User Customers ("**McAfee Enterprise Personal Data**").

The details of the processing activities to be carried out by the Supplier under the Agreement and, the special categories of Personal Data where applicable, are specified in Appendix 1 of Schedule 1.

2. OBLIGATIONS OF THE SUPPLIER

The Supplier agrees and warrants:

(a) to process Personal Data only:

- on behalf of McAfee Enterprise and in accordance with its documented instructions unless otherwise required by Data Protection Laws;
- for the sole purpose of executing the Agreement or as otherwise instructed by McAfee, and not for the Supplier's own purposes or other commercially exploitation. For clarity, Supplier will not collect, retain, use, or disclose McAfee Enterprise Personal Data for any purpose other than as necessary for the specific purpose of processing McAfee Enterprise Personal Data, including collecting, retaining, using, or disclosing McAfee Enterprise Personal Data for a commercial purpose other than providing and enhancing McAfee Enterprise Products and Services. This provision shall not apply to anonymized DDoS and traffic statistics that may be collected as long as such data is not reasonably related to, directly or in combination with other data, McAfee Enterprise Personal Data. Supplier will not use McAfee Enterprise Personal Data for the purpose of providing services to another person or entity except for the sole purposes of detecting data security incidents and protecting against fraudulent or illegal activity. Without limiting the foregoing, Supplier will not sell McAfee Enterprise Personal Data; and
- in compliance with this Data Processing Agreement; and
- in an encrypted and anonymized manner as, necessary while in transit and storage and in accordance with the current state of the art encryption technology as available in the commercial marketplace;

(b) if it is legally required to process McAfee Enterprise Personal Data otherwise than as instructed by McAfee, to notify McAfee Enterprise and the Data subject before such processing occurs, unless the Data Protection Law requiring such processing prohibits the Supplier from notifying McAfee Enterprise on an important ground of public interest, in which case it shall notify McAfee Enterprise as soon as that Data Protection Law permits it to do so; and to take legal action against any disclosure of Personal Data and to refrain

from disclosing the Personal Data to authorities or other third parties until a competent court of last instance has ordered the personal data to be disclosed.

(c) that it has implemented and will maintain appropriate technical and organisational measures in accordance with those described in the International Organization for Standardization (ISO 27001, IS0 27018 or its equivalent or superseding standard if applicable) to protect McAfee Enterprise Personal Data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access and, in particular, where the processing involves the transmission of data over a network, against all other unlawful forms of processing.

Having regard to the state of the art and cost of their implementation, the Supplier agrees that such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of McAfee Enterprise Personal Data to be protected and will at a minimum include those measures described under the SCCs incorporated herein by reference, and under Article 32 of the GDPR and Articles 33, 36 to 38 Regulation (EU) 2018/1725;

(d) that protective devices are set up for ensuring the integrity and the authenticity of McAfee Enterprise Personal Data, especially the state-of-the-art protective devices against malware and similar security attacks;

(e) that it has implemented measures to prevent McAfee Enterprise Personal Data from undergoing any unwanted degradation or deletion without having a copy immediately usable;

(f) that it has a business continuity plan which includes measures to reduce unavailability of the services in the event of a lasting incident or security breach, and which includes service levels and maximum recovery response and resolution time charter to face any crisis scenario;

(g) that it will treat all McAfee Enterprise Personal Data as confidential information and not disclose such confidential information without McAfee's prior written consent except:

- to those of its personnel who need to know the confidential information in order to carry out the Services; and
- where it is required by a court to disclose McAfee Enterprise Personal Data, or where there is a statutory obligation to do so, but only to the minimum extent necessary to comply with such court order or statutory obligation;

(h) to take reasonable steps to ensure that its personnel who have access to the Personal Data:

- are subject to a code of conduct and an ethic guide substantially compliant with McAfee's code of conduct available at **https://www.mcafee.com/us/resources/misc/code-of-conduct.pdf**;
- are informed of the confidential nature of McAfee Enterprise Personal Data and obliged to keep such McAfee Enterprise Personal Data confidential; and
- are aware of and comply with the Supplier's duties and their personal duties and obligations under this Data Processing Agreement;

(i) that it will promptly, and at least within **24 hours**, notify McAfee Enterprise about:

- any instruction which, in its opinion, infringes applicable law;
- any actual or suspected security breach, unauthorised access, misappropriation, loss, damage or other compromise of the security, confidentiality, or integrity of McAfee Enterprise Personal Data processed by Supplier or a Subprocessor ("Security Breach");
- any complaint, communication or request received directly by the Supplier or a Subprocessor from a data subject and pertaining to their Personal Data, without responding to that request unless it has been otherwise authorised to do so by McAfee; and
- any change in legislation applicable to the Supplier or a Subprocessor which is likely to have a substantial adverse effect on the warranties and obligations set out in this DPSA;

(j) that upon discovery of any Security Breach, it shall:

- immediately take action to prevent any further Security Breach; and
- provide McAfee Enterprise with full and prompt cooperation and assistance in relation to any notifications that McAfee Enterprise is required to make as a result of the Security Breach;

(k) to provide McAfee Enterprise with full and prompt cooperation, at least **within 48 hours**, and assistance in relation to any complaint, communication or request received from a Data Subject, including by:

- providing McAfee Enterprise with full details of the complaint, communication or request;
- where authorised by McAfee, complying with a request from a data subject in relation to their McAfee Enterprise Personal Data within the relevant timescales set out by applicable law and in accordance with McAfee's instructions;
- providing McAfee Enterprise with any McAfee Enterprise Personal Data it holds in relation to a Data Subject, if required in a commonly-used, structured, electronic and machine-readable format;
- providing McAfee Enterprise with any information requested by McAfee Enterprise relating to the processing of McAfee Enterprise Personal Data under this DPSA;
- correcting, deleting or blocking any McAfee Enterprise Personal Data; and
- implementing appropriate technical and organisational measures that enable it to comply with this subsection k;
- ensuring that the data subject has been informed or will be informed before, or as soon as possible after, their Personal Data is transmitted to a third country not providing adequate protection within the meaning of Applicable Laws;

(l) to provide McAfee Enterprise with full and prompt cooperation and assistance in relation to any data protection impact assessment or regulatory consultation that McAfee Enterprise is legally required to make in respect of McAfee Enterprise Personal Data;

(m) to appoint, and identify to McAfee, an individual to support McAfee Enterprise in monitoring compliance with this DPSA and to make available to McAfee Enterprise upon request all information and evidence necessary to demonstrate that the Supplier is complying with its obligations under this DPSA;

(n) at the request of McAfee, to submit its data processing facilities for audits and inspections of the processing activities covered by this DPSA, which shall be carried out by McAfee Enterprise or a regulated End-User Customer (i.e. when a government or regulatory body with binding authority ("Regulator") regulates such entity's regulated services such as banking for instance) or any independent or impartial inspection agents or auditors selected by McAfee Enterprise or a regulated End-User Customer and not reasonably objected to by the Supplier, and to allow McAfee Enterprise to provide any such reports to its End-User Customers where required.

(o) that it shall maintain the list attached hereto as Appendix 3 of subprocessors that may Process the Personal Data of Supplier's customers. Supplier shall require all subprocessors to abide by the same obligations as Supplier under this Agreement. Supplier remains responsible at all times for compliance with the terms of this Agreement by Supplier Affiliates and subprocessors. McAfee Enterprise consents to Supplier's use of Supplier's Affiliates and subprocessors in the performance of the Services. Supplier shall inform McAfee Enterprise of any new subprocessors Supplier intends to engage and will obtain prior written consent from McAfee. McAfee Enterprise may object to the engagement of any new Subprocessor but shall not unreasonably withheld its consent to such appointment; Supplier shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s).

(p) upon request, to promptly send a copy of any data privacy, data protection (including, but not limited to, measures and certifications) and confidentiality portions of an agreement it concludes with a Subprocessor relating to McAfee Enterprise Personal Data to McAfee Enterprise;

(q) shall promptly notify McAfee should Supplier receive a request from a data subject to have access to Personal Data or any complaint or request relating to McAfee Enterprise 's obligations under applicable Data Protection Laws. McAfee Enterprise is solely responsible for responding to such request unless Supplier does not inform McAfee Enterprise of the request, and Supplier will not respond to any such data subject unless required by applicable laws or unless instructed in writing by McAfee Enterprise to do so;

(r) has no reason to believe that the laws and practices in the third country of destination applicable to the processing of the Personal Data, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not

exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses;

(s) shall document the assessment under Clause 15 paragraph (b) of the SCCs and make it available to the competent supervisory authority on request of McAfee.

3. LIABILITY. Supplier shall remain fully liable to McAfee Enterprise for any subprocessors' processing of McAfee Enterprise Personal Data under the Agreement. Notwithstanding anything contained in the Agreement to the contrary, nothing in the limitation of liability in the Agreement will be read or interpreted in any way to limit Supplier's liability for breach of this DPSA.

4. INTERNATIONAL DATA TRANSFER.

Without prejudice to any applicable Data Protection laws, no Transfer of Personal Data may take place to countries that have not received an Adequacy Decision or without having in place a Transfer Mechanism.

Restricted transfers from the EEA. Where the Transfer to Supplier is covered by Supplier's BCR, Supplier warrants that it shall (i) promptly notify McAfee Enterprise of any subsequent material changes in such authorization, and (ii) downstream any of its obligations under its Supplier BCRs to Sub-processors by entering into an appropriate onward transfer agreement with any such Sub-processor, or by entering into SCCs. To the extent the Transfer is not covered by BCRs, any Transfer will be governed by unmodified SCCs incorporated herein by reference, and the Appendices attached hereto (Schedule 1).

Restricted Transfers from Argentina. To the extent a Transfer involves Argentinian Personal Data to Supplier or its Sub-processors located outside Argentina, such Transfer will be governed by the Argentine Model Clauses incorporated herein by reference and its Appendix attached hereto (Schedule 2).

Restricted transfers from other jurisdictions. Transfers from other jurisdictions globally that have Transfer restrictions are subject to the terms of this Data Processing Exhibit or to the mandatory terms required under local Applicable Laws of such Transfer restrictions documentation (such as – but not limited to - the MCCs), including any data protection and security policies referenced herein.

Sub-processors. Supplier will provide without undue delay McAfee Enterprise with a copy of the relevant Transfer Mechanism and/or related Data Processor provisions with its Sub-processors upon request. McAfee Enterprise shall be entitled to terminate the Agreement if the approved Transfer Mechanism is invalidated and no alternative approved Transfer Mechanism is put in place or when the related Data Processing provisions with its Sub-processors do not comply with this Data Protection Exhibit.

In the event of inconsistencies between the provisions of the Transfer Mechanisms and this Data Processing Exhibit or the Agreement, said Transfer Mechanisms shall take precedence

to the extent required by Data Protection Laws. In the event that such Transfer Mechanisms are amended, replaced or repealed under Data Protection Laws or in the event new Transfer Mechanisms terms are adopted under Data Protection Laws, the parties shall deem such Transfer Mechanisms deemed as incorporated herein by reference, and shall work together in good faith to enter into any required updated version or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws. This Data Processing Exhibit supersedes any and all prior understandings and agreements relating to the protection of data and compliance with Data Protection Laws and the express provisions of this Data Processing Exhibit control over any other agreement or amendment.

5. INDEMNITY. The Supplier shall indemnify and keep indemnified and defend at its own expense McAfee Enterprise against all costs, claims, damages or expenses incurred by McAfee Enterprise or for which McAfee Enterprise may become liable due to any failure by the Supplier or its employees or agents to comply with any of its obligations under this DPSA.

Additional Terms for Individual Remedies. To the extent required under local applicable Data Protection Laws, Supplier and its sub-processors will provide data subjects with direct rights of enforcement of the Transfer Mechanisms.

6. ALLOCATION OF COSTS. Each party shall perform its obligations under this DPSA at its own cost.

7. TERM AND TERMINATION OF THE SERVICES.

The parties agree that McAfee Enterprise Personal Data will be processed by the Supplier for the duration of the Services under the Agreement.

The parties agree that upon termination of the Services in so far as they relate to McAfee Enterprise Personal Data, the Supplier and all subprocessors shall, at the choice of McAfee Enterprise , return all McAfee Enterprise Personal Data and the copies thereof to McAfee Enterprise , or securely destroy all McAfee Enterprise Personal Data and certify to McAfee Enterprise that it or they have done so, unless Data Protection Laws to which the Supplier or a Subprocessor are subject prevent the Supplier or Subprocessor from returning or destroying all or part of McAfee Enterprise Personal Data. In such a case, the Supplier warrants that it will guarantee the confidentiality of McAfee Enterprise Personal Data and will not actively process McAfee Enterprise Personal Data anymore and will guarantee the return and/or destruction of McAfee Enterprise Personal Data as requested by McAfee Enterprise when the legal obligation to not return or destroy the information is no longer in effect.

8. RECORDS AND PROOFS.

Supplier warrants it keeps records concerning its security, and organizational technical measures as well as records on any security incident affecting McAfee Enterprise Personal Data. Such records shall be made available in a standard format immediately exploitable

and available for inspection, upon McAfee Enterprise 's request in the course of a security check or in the framework of an audit.

9. TERM, PORTABILITY AND REVERSIBILITY AND SURVIVAL

This DPSA shall remain in full force as long as the Services Agreement remains in full force. In order to ensure portability of the Personal Data, and should the Services Agreement be terminated for any reason, Supplier shall, within five (5) days of McAfee Enterprise 's request, make available McAfee Enterprise Personal Data in a standard format. Such Information shall include account level information including IP addresses, hostnames, infrastructure information and McAfee Enterprise contact information.

Survival. Any terms of this DPSA which by their nature should survive the termination of this DPSA shall survive such termination, including, without limitation, the indemnity and liability terms herein.

10. Standard Contractual Clauses.

By executing this DPSA, Supplier is deemed to execute the Standard Contractual Clauses as set out in full on our website, which will have legally binding force on the parties. A link to the Standard Contractual Clauses can be found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

11. MISCELLANEOUS.

In the event of inconsistencies between the provisions of this DPSA and the Services Agreement, the provisions of this DPSA shall prevail with regard to the parties' data protection obligations relating to McAfee Enterprise Personal Data. In cases of doubt, this DPSA shall prevail, in particular, where it cannot be clearly established whether a clause relates to a party's data protection obligations.

Should any provision or condition of this DPSA be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this DPSA shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this DPSA to the maximum extent permitted by law. The provision or condition affected shall be construed either: (i) to be amended in such a way that ensures its validity, lawfulness and enforceability while preserving the parties' intentions, or if that is not possible, (ii) as if the invalid, unlawful or unenforceable part had never been contained in this DPSA.

Any amendments to this DPSA shall be in writing duly signed by authorised representatives of the parties hereto.

12. BCRs.

If at any time after the Effective Date, McAfee Enterprise elects to use BCRs, McAfee Enterprise shall transfer Personal Data in accordance with its BCR, and McAfee Enterprise

will be regarded as the Data Exporter and the Supplier will be regarded as the Data Importer. Once approved, McAfee Enterprise shall maintain such BCR's throughout the term of the Agreement. Should McAfee Enterprise cease to abide by such BCR's, the Parties will agree not to transfer any Personal Data outside the appropriate mechanisms provided under Sections 44 through 50 of the GDPR.

-Schedule 1 follows this page-

Signature:

SCHEDULE 1

Appendices to the Standard Contractual Clauses: Module 2

APPENDIX 1 OF SCHEDULE 1 - DESCRIPTION OF THE PARTIES (MODULE 2)

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 Musarubra Ireland Limited 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.

APPENDIX 2 OF SCHEDULE 1 - DESCRIPTION OF THE TRANSFERS (MODULE 2)

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.

☒ 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.

Frequency of the transfer: (the frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis). Please tick as applicable.

☐ None.

☐ One-off.

☐ On-going.

☐ In accordance with the specifications described under the Agreement.

Period of retention: please provide the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

☐ Limited to the term of the Agreement.

☐ Other. Please specify _____

☐ criteria used to determine that period. Please specify : _____

.

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

- Subject matter:
- Nature:
- Duration:

Competent supervisory authority:

☐ Data Protection Commission of Ireland

☐ Other. Please specify: _____

-Appendix 3 to Schedule 1 follows this page-

APPENDIX 3 OF SCHEDULE 1

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Appendix 3 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 Services Agreement, Supplier shall comply with the following, unless otherwise indicated below and approved by McAfee Enterprise .

1. Introduction

These **Supplier Security and Privacy Requirements** ("SSPRs") establish Supplier's minimum-security standards for protection of McAfee Enterprise Confidential Information, including McAfee Enterprise 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 Enterprise . 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 Enterprise or on behalf of McAfee Enterprise 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 Enterprise 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 Enterprise . 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 Enterprise 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 Enterprise may have included important updates/changes from previous versions. If a Supplier, its 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 Enterprise 's Information Security team shall evaluate a Supplier's security capability. If approved by McAfee Enterprise , 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.

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 pseudonymisation 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 organisational 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 Enterprise Confidential Information subject to the prior written approval of McAfee Enterprise and must be certified to ISO 27001 standards as a minimum. McAfee Enterprise reserves the right to perform a security review and risk assessment of applications and services containing McAfee Enterprise 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 Enterprise Confidential Information must first be reviewed and approved by McAfee Enterprise Information Security Department. Applications that require physical separation cannot be on a cloud-based service unless duly segregated and approved in writing by McAfee Enterprise . Supplier shall ensure McAfee Enterprise 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 Enterprise or a regulated End-User Customer, to audit Supplier and Supplier agrees to allow McAfee Enterprise to provide any such reports to its End-User Customers where required.

4. Vulnerability Management

If Supplier is hosting a public-facing McAfee Enterprise website, Supplier shall perform daily vulnerability scans on all internet facing web sites where McAfee Enterprise has branded content,

McAfee Enterprise is the primary site owner or 'McAfee Enterprise ' is part of the URL. McAfee Enterprise uses the McAfee Enterprise 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 Enterprise will not charge Supplier for the McAfee Enterprise Secure scanning service. McAfee Enterprise 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 Enterprise threat rating [5] or [4] must be remediated in 1 to 5 calendar days; (ii) High, McAfee Enterprise threat rating [3] must be remediated within 10 calendar days and (iii) Medium, McAfee Enterprise threat rating [2] must be remediated within 30 calendar days.

If the security vulnerabilities identified by the McAfee Enterprise vulnerability scanning process have not been addressed in the above timelines, McAfee Enterprise 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 Enterprise compliance. McAfee Enterprise considers a web site compliant when McAfee Enterprise security standards are met. McAfee Enterprise will notify Suppliers any time the McAfee Enterprise 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.

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	
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	ISO 27001 A.12.7.1	

	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 Enterprise (e.g., ISO27001, PCI-DSS or 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 Enterprise 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	
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	
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	

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	
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	
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	
IT Asset Management ▪ All data provided by McAfee Enterprise 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	
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	
Return of IT Assets	Upon termination of employment, end users return all company-owned IT assets	ISO 27001 A.8.1.4	
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	

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	
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	

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	
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	

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	
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	
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	

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	
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	
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	

Operational Security

- Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
- All data provided by McAfee Enterprise 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	

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	
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	
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	
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	
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	

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	
Encryption of Data	Sensitive information shall be encrypted during transmission	ISO 27001 A.13.2.1	

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 Enterprise and/or a McAfee Enterprise website must be reported to McAfee Enterprise . Notification must be within 48 hours from detection if McAfee Enterprise data, the McAfee Enterprise brand, logo or trademarks are involved or compromised.
- Any security event where a McAfee Enterprise website had unauthorized access or was compromised must be reported to McAfee Enterprise .
- 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 Enterprise 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	
Employee Reporting	Employees/contractors have mechanisms available to report potential incidents or security weaknesses observed		

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 Enterprise 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	

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 Enterprise 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 Enterprise classification of "Confidential". (d) Existing services containing confidential data may not be pushed to the cloud or transferred to cloud service vendors without McAfee Enterprise approval. It is subject to approval following a Security review and Risk Assessment by McAfee Enterprise .

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 Enterprise requires daily vulnerability scans performed on all internet facing web sites where McAfee Enterprise has branded content and is the primary site owner or 'McAfee Enterprise ' is part of the URL. McAfee Enterprise uses the McAfee Enterprise 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 Enterprise does not charge the Supplier for the McAfee Enterprise Secure scanning service.
- McAfee Enterprise requires daily access to the reports.
- Upon identification of security vulnerabilities in a production application, the Supplier must remediate within the following time lines:
    - Critical: 7 days
    - High: 30 days
    - Medium: 90 days
    - Low: 180 days
- If the security vulnerabilities identified by the McAfee Enterprise vulnerability scanning process have not been addressed in the above timelines, McAfee Enterprise 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 Enterprise compliance.
- McAfee Enterprise considers a web site compliant when McAfee Enterprise security standards are met. McAfee Enterprise Security will notify Suppliers of each of the McAfee Enterprise 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 Enterprise .
- 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 Enterprise 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 Enterprise scanning of McAfee Enterprise Web applications. McAfee Enterprise 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 Enterprise data is Confidential.

10.2 Privacy Management

- Applications such as "Software as a Service' used by McAfee Enterprise to collect Personal Data must have the URL for the McAfee Enterprise 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 Enterprise Confidential, McAfee Enterprise Confidential – Internal Use Only or McAfee Enterprise 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 Enterprise must be through secure communications.
- All data exchanged with McAfee Enterprise for mission or business critical functions, (B2B), require secure intercompany communications (ICC) implemented by McAfee Enterprise IT Engineering services. The McAfee Enterprise program manager is responsible for communications funding and will arrange for Suppliers to engage with the McAfee Enterprise 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 Enterprise Information Security.

13. Duration

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

-Appendix 4 of Schedule 1 follows this page-

APPENDIX 4 OF SCHEDULE 1

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 follows this page-

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: