McAfee's Standard Contractual Clauses for Customers

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

Standard Contractual Clauses: C-to-P Transfer

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**

i. 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.

ii. 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.

iii. 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.

iv. 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**

i. 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.

ii. 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.

iii. 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**

i. 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.

ii. 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**

i. 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.

ii. 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.

iii. 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**

i. 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.

ii. 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.

iii. 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.

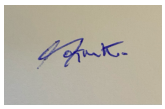
iv. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. **OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES**

i. 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.

ii. 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 importer:
Name (written out in full): Roy Kamp
Position: Data Protection Officer
Address: McAfee, LLC on behalf of McAfee Ireland Limited and all other Affiliates
6220 America Center Drive San Jose, CA 95002. USA

Signature: 

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Signature:

SCHEDULE 1 – EXHIBITS TO THE SCCS

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 (i) the company that has executed the Standard Contractual Clauses as a Data Exporter and (ii) all Customer's Affiliates (as defined under the Agreement) established within the European Economic Area (EEA) and Switzerland that export Personal Data under the Agreement.

Data importer

The Data Importer is McAfee LLC on behalf of McAfee Ireland Limited and other McAfee Affiliates. The Data Importer provides products and services to the Data Exporter in relation to security products and services under the Agreement between the Data Exporter and the Data Importer, 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.

☒ Employees of Corporate customers

☐ McAfee consumer customers and former consumer customers

☒ McAfee Sub-processor's contacts

Categories of data

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

☐ Employees' names and contact information, including home 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.

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

☐ McAfee Consumer customers' names and business contact information, including addresses, emails, phone numbers, IP addresses.

☒ McAfee Sub-processors' contacts, including employees' names and business contact information, including addresses, emails, phone numbers, IP addresses.

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 specify):

☐ The Personal Data will be used to provide human resources benefits.

☒ The Personal Data will be used to provide information technology services to the Customer employees.

☒ The Personal Data will be used to provide security and data protection Services.

☒ The Personal Data will be used to enhance McAfee's threat defences.

☒ The Personal Data will be used to provide Customer with Services.

☒ The Personal Data will be used to provide licenses to McAfee products and Services.

APPENDIX 2 OF SCHEDULE 1
Technical and Organisational Security Measures

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).

McAfee's Information Security Management System (ISMS) is centrally managed from Plano, Texas by the Information Security Governance & Assurance Group. The scope of the McAfee ISMS governs the management of information security across all global locations and services, defined data centres, and is inclusive of the following sites with primary security operations:

- •McAfee, LLC. - 5000 Headquarters Drive, Plano, Texas 75024-5826 USA;
- •McAfee Ireland Limited - Building 2000, Citygate, Mahon, Cork City, Ireland.

In addition to any data security requirements set forth in the DPA, McAfee shall comply with the following:

Standard	Control Ref/ Title		Control Description
ISO 27001 - Information Security Management System ***(incl. controls expanded for ISO 27017/27018)***	***6.1.3 - A.5 Information Security Policy***		
	5.1.1	Policies for information security	A set of policies for information security is defined, approved by management, published and communicated to employees and relevant external parties.
	5.1.2	Review of the policies for information security	The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
	6.1.3 - A.6 Organization of Information Security		
	6.1.1	Information security roles and responsibilities	All information security responsibilities are defined and allocated.
	6.1.2	Segregation of duties	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
	6.1.3	Contact with authorities	Appropriate contacts with relevant authorities are maintained.
	6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.
	6.1.5	Information security in project management	Information security is addressed in project management, regardless of the type of the project.
	6.2.1	Mobile device policy	A policy and supporting security measures is adopted to manage the risks introduced by using mobile devices.
	6.2.3	Teleworking	A policy and supporting security measures is implemented to protect information accessed, processed or stored at teleworking sites.
	6.1.3 - A.7 Human Resource Security		
	7.1.1	Screening	Background verification checks on all candidates for employment is carried out in accordance with relevant laws, regulations and ethics and is proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
	7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors state their and the organization's responsibilities for information security.
	7.2.1	Management responsibilities	Management requires all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
	7.2.2	Information security awareness, education, training	All employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
	7.2.3	Disciplinary process	There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
	7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor and enforced.
	6.1.3 - A.8 Asset Management		
	8.1.1	Inventory of assets	Assets associated with information and information processing facilities are identified and an inventory of these assets shall be drawn up and maintained.
	8.1.2	Ownership of assets	Assets maintained in the inventory are owned.
	8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and

			implemented.
	8.1.4	Return of assets	All employees and external party users return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
	8.2.1	Classification of information	Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
	8.2.2	Labelling of information	An appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.2.3	Handling of assets	Procedures for handling assets is developed and implemented in accordance with the information classification scheme adopted by the organization.
	8.3.1	Management of removal media	Procedures is implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
	8.3.2	Disposal of media	Media is disposed of securely when no longer required, using formal procedures.
	8.3.3	Physical media transfer	Media containing information is protected against unauthorized access, misuse or corruption during transportation.
	6.1.3 - A.9 Access Control		
	9.1.1	Access control policy	An access control policy is established, documented and reviewed based on business and information security requirements.
	9.1.2	Access to networks and network services	Users are only provided with access to the network and network services if they have been specifically authorized to use such services.
	9.2.1	User registration and de-registration	A formal user registration and de-registration process is implemented to enable assignment of access rights.
	9.2.2	User access provisioning	A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.
	9.2.3	Management of privileged access rights	The allocation and use of privileged access rights is restricted and controlled.
	9.2.4	Management of secret authentication info of users	The allocation of secret authentication information is controlled through a formal management process.
	9.2.5	Review of user access rights	Asset owners review users' access rights at regular intervals.
	9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.
	9.3.1	Use of secret authentication information	Users are required to follow the organization's practices in the use of secret authentication information.
	9.4.1	Information access restriction	Access to information and application system functions is restricted in accordance with the access control policy.
	9.4.2	Secure log on procedures	Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure.
	9.4.3	Password management system	Password management systems is interactive and ensures quality passwords.
	9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.
	9.4.5	Access control to program source code	Access to program source code is restricted.
	6.1.3 - A.10 Cryptography		
	10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information is developed and implemented.
	10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys is developed and implemented through their whole lifecycle.
	6.1.3 - A.11 Physical and Environmental Security		
	11.1.1	Physical security perimeter	Security perimeters is defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
	11.1.2	Physical entry controls	Secure areas is protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
	11.1.3	Securing offices, rooms, facilities	Physical security for offices, rooms and facilities are designed and applied.
	11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents are designed and applied.

	11.1.5	Working in secure areas	Procedures for working in secure areas are designed and applied.
	11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
	11.2.1	Equipment siting and protection	Equipment are sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	11.2.2	Supporting utilities	Equipment are protected from power failures and other disruptions caused by failures in supporting utilities.
	11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage.
	11.2.4	Equipment maintenance	Equipment are correctly maintained to ensure its continued availability and integrity.
	11.2.5	Removal of assets	Equipment, information or software are not taken off-site without prior authorization.
	11.2.6	Security of equipment and assets off-premises	Security is applied to off-site assets taking into account the different risks of working outside the organization's premises.
	11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media is verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
	11.2.8	Unattended user equipment	Users ensure that unattended equipment has appropriate protection.
	11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.
	6.1.3 - A.12 Operations Security		
	12.1.1	Documented operating procedures	Operating procedures are documented and made available to all users who need them.
	12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security are controlled.
	12.1.3	Capacity management	The use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
	12.1.4	Separation of development, testing & operational environments	Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.
	12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware are implemented, combined with appropriate user awareness.
	12.3.1	Information backup	Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
	12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.
	12.4.2	Protection of log information	Logging facilities and log information are protected against tampering and unauthorized access
	12.4.3	Administrator and operator logs	System administrator and system operator activities are logged, and the logs are protected and regularly reviewed.
	12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain are synchronized to a single reference time source.
	12.5.1	Installation of software on operational systems	Procedures are implemented to control the installation of software on operational systems.
	12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used are obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
	12.6.2	Restrictions on software installation	Rules governing the installation of software by users are established and implemented.
	12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes.
	6.1.3 - A.13 Communications Security		
	13.1.1	Network controls	Networks are managed and controlled to protect information in systems and applications.
	13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all

			network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.
	13.1.3	Segregation in networks	Groups of information services, users and information systems are segregated on networks.
	13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.
	13.2.2	Agreements on information transfer	Agreements address the secure transfer of business information between the organization and external parties.
	13.2.3	Electronic messaging	Information involved in electronic messaging is appropriately protected.
	13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information are identified, regularly reviewed and documented.
	6.1.3 - A.14 Systems Acquisition, Dev. & Maintenance		
	14.1.1	Information security requirements analysis & specification	The information security related requirements are included in the requirements for new information systems or enhancements to existing information systems.
	14.1.2	Securing application services on public networks	Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
	14.1.3	Protecting application services transactions	Information involved in application service transactions is protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
	14.2.1	Secure development policy	Rules for the development of software and systems are established and applied to developments within the organization.
	14.2.2	System change control procedures	Changes to systems within the development lifecycle are controlled by the use of formal change control procedures.
	14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.
	14.2.4	Restrictions on changes to software packages	Modifications to software packages are discouraged, limited to necessary changes and all changes are strictly controlled.
	14.2.5	Secure system engineering principles	Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.
	14.2.6	Secure development environment	secure development environments are established and are appropriately protected for system development and integration efforts to cover the entire system development lifecycle
	14.2.7	Outsourced development	The organization supervises and monitors the activity of outsourced system development.
	14.2.8	System security testing	Testing of security functionality is carried out during development.
	14.2.9	System acceptance testing	Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.
	14.3.1	Protection of test data	Test data is selected carefully, protected and controlled.
	6.1.3 - A.15 Supplier Relationship		
	15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets are agreed with the supplier and documented.
	15.1.2	Addressing security within supplier agreements	All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information
	15.1.3	Information communication technology supply chain	Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.
	15.2.1	Monitoring and review of supplier services	Supplier service delivery is regularly monitored, reviewed and audited.
	15.2.2.	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

	6.1.3 - A.16.1.3 Information Security Incident Management		
	16.1.1	Responsibilities and procedures	Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.
	16.1.2	Reporting information security events	Information security events are reported through appropriate management channels as quickly as possible.
	16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.
	16.1.4	Assessment of and decision on information security events	Information security events are assessed and are decided if they are to be classified as information security incidents.
	16.1.5	Response to information security incidents	Information security incidents are responded to in accordance with the documented procedures.
	16.1.6	Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents are used to reduce the likelihood or impact of future incidents.
	16.1.7	Collection of evidence	Procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence are defined and applicable.
	6.1.3 - A.17 Information Security Aspects of Business Continuity Management		
	17.1.1	Planning information security continuity	Requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster are determined.
	17.1.2	Implementing information security continuity	Processes and procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented and maintained.
	17.1.3	Verify, review and evaluate information security continuity	Established and implemented information security continuity controls are verified at regular intervals in order to ensure that they are valid and effective during adverse situations.
	17.2.1	Availability of information processing facilities	Information processing facilities are implemented with redundancy sufficient to meet availability requirements.
	6.1.3 - A.18 Compliance		
	18.1.1	Identification of applicable legislation & contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are explicitly identified, documented and kept up to date for each information system and the organization.
	18.1.2	Intellectual property rights	Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
	18.1.3	Protection of records	Records are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislation, regulatory, contractual and business requirements.
	18.1.4	Privacy and protection of Personal Data	Privacy and protection of personally identifiable information (Personal Data) are ensured as required in relevant legislation and regulation where applicable.
	18.1.5	Regulation of cryptographic controls	Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations.
	18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.
	18.2.2	Compliance with security policies & standards	Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
	18.2.3	Technical compliance review	Information systems are regularly reviewed for compliance with the organization's information security policies and standards
ISO 27017 - Security Controls for Cloud Services	**CLD.6.3 - Relationship between cloud service customer & provider**		
	6.3.1	Shared roles & responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service are allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.
	8.1.5	Removal of cloud service customer assets	Removal of cloud service customer assets
	CLD.9.5 - Access control of CSP data in		

	shared virtual environment		
	9.5.1	Segregation in virtual computing environments	A cloud service customer's virtual environment running on a cloud service is protected from other cloud service customers and unauthorized persons.
	9.5.2	Virtual machine hardening	Virtual machines in a cloud computing environment are hardened to meet business needs.
	12.1.5	Administrator's operational security	Procedures for administrative operations of a cloud computing environment are defined, documented and monitored.
	12.4.5	Monitoring of cloud services	The cloud service customer has the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.
	13.1.4	Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks is verified based on the cloud service provider's network security policy.
ISO 27018 - Protection of Personal Data in Public Clouds, Acting as Personal Data Processors	**A.2 - Consent and choice**		
	A.2.1	Obligation to co-operate regarding Personal Data principals' rights	The public cloud Personal Data processor can provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of Personal Data principals' rights to access, correct and/or erase Personal Data pertaining to them.
	A.3 - Purpose legitimacy and specification		
	A.3.1	Public cloud Personal Data processor's purpose	Personal Data to be processed under a contract is not processed for any purpose independent of the instructions of the cloud service customer.
	A.3.2	Public cloud Personal Data processor's commercial use	Personal Data processed under a contract is not used by the public cloud Personal Data processor for the purposes of marketing and advertising without express consent. Such consent is not a condition of receiving the service
	A.5 - Data minimization		
	A.5.1	Secure erasure of temporary files	Temporary files and documents are erased or destroyed within a specified, documented period
	A.6 - Use, retention, and disclosure limitation		
	A.6.1	Personal Data disclosure notification	The contract between the public cloud Personal Data processor and the cloud service customer requires the public cloud Personal Data processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of Personal Data by a law enforcement authority, unless such a disclosure is otherwise prohibited
	A.6.2	Recording of Personal Data disclosure	Disclosures of Personal Data to third parties is recorded, including what Personal Data has been disclosed, to whom and at what time.
	A.8 - Openness, transparency, and notice		
	A.8.1	Disclosure of sub-contracted Personal Data processing	The use of sub-contractors by the public cloud Personal Data processor to process Personal Data is disclosed to the relevant cloud service customers before their use.
	A.10 - Accountability		
	A.10.1	Notification of a data breach involving Personal Data	The public cloud Personal Data processor promptly notifies the relevant cloud service customer in the event of any unauthorized access to Personal Data or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of Personal Data.
	A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures are retained for a specified, documented period upon replacement (including updating).
	A.10.3	Personal Data return, transfer and disposal	The public cloud Personal Data processor have a policy in respect of the return, transfer and/or disposal of Personal Data and make this policy available to the cloud service customer
	A.11 - Information security		
	A.11.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud Personal Data processor's control with access to Personal Data are subject to a confidentiality obligation.
	A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying Personal Data is restricted.
	A.11.3	Control and logging of data restoration	There is a procedure for, and a log of, data restoration efforts.

	A.11.4	Protecting data on storage media leaving the premises	Personal Data on media leaving the organization's premises is subject to an authorization procedure and is not accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).
	A.11.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption cannot be used except where it is unavoidable, and any use of such portable media and devices is documented.
	A.11.6	Encryption of Personal Data transmitted over public data-transmission networks	Personal Data that is transmitted over public data-transmission networks is encrypted prior to transmission
	A.11.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.
	A.11.8	Unique use of user IDs	If more than one individual has access to stored Personal Data, then they each have a distinct user ID for identification, authentication and authorization purposes
	A.11.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained.
	A.11.10	User ID management	De-activated or expired user IDs are not be granted to other individuals.
	A.11.11	Contract measures	Contracts between the cloud service customer and the public cloud Personal Data processor specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures are not subject to unilateral reduction by the public cloud Personal Data processor
	A.11.12	Sub-contracted Personal Data processing	Contracts between the public cloud Personal Data processor and any sub-contractors that process Personal Data specify minimum technical and organizational measures that meet the information security and Personal Data protection obligations of the public cloud Personal Data processor. Such measures are not subject to unilateral reduction by the sub-contractor.
	A.11.13	Access to data on pre-used data storage space	The public cloud Personal Data processor ensures that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.
	A.12 - Privacy compliance		
	A.12.1	Geographical location of Personal Data	The public cloud Personal Data processor specifies and document the countries in which Personal Data might possibly be stored.
	A.12.2	Intended destination of Personal Data	Personal Data transmitted using a data-transmission network is subject to appropriate controls designed to ensure that data reaches its intended destination.
PCI-DSS	1	Firewall configuration to protect cardholder data	The installation contains a formal process for approving and testing all network connections and changes to the firewall and router configurations and complies with PCI-DSS standards. The firewall and router configurations restrict connections between untrusted networks and any system components in the cardholder data environment and prohibit direct public access between the Internet and any system component in the cardholder data environment. Security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties and include a personal firewall software.
	2	Do not use vendor-supplied defaults for system passwords and other security parameters	Vendor-supplied defaults are changed, and McAfee removes or disables unnecessary default accounts before installing a system on the network. The configuration complies with standards that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. All non-console administrative access is encrypted using strong cryptography. Security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties
	3	Protect stored cardholder data	Cardholder data storage is kept to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage. Sensitive authentication data after authorization (even if encrypted) is not stored.
	4	Encrypt transmission of cardholder data across open, public networks	Use of strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public network.

	5	Use and regularly update anti-virus software or programs.	All anti-virus mechanisms are maintained as follows: - Are kept current, - Perform periodic scans - Generate audit logs which are retained per PCI DSS Requirement 10.7.
	6	Develop and maintain secure systems and applications	security vulnerabilities are identified, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
	7	Restrict access to cardholder data by business need to know	Access to system components and cardholder data is limited to only those individuals whose job requires such access.
	8	Assign a unique ID to each person with computer access	User Management procedures are defined and implemented to ensure proper user identification management for non-consumer users and administrators on all system components as follows:
	9	Restrict physical access to cardholder data	Facility entry controls are used to limit and monitor physical access to systems in the cardholder data environment.
	10	Track and monitor all access to network resources and cardholder data	Audit trails are implemented to link all access to system components to each individual user.
	11	Regularly test security systems and processes	Processes are implemented to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
	12	Maintain a policy that addresses information security for all personnel	A security policy is established, published, maintained, and disseminated.

Appendix 3 of SCHEDULE 1 - Authorized Third-Party Sub-processors

The current list of McAfee's Sub-processors is provided under https://www.mcafee.com/enterprise/en-us/assets/legal/enterprise-sub-processor-list.pdf.

SCHEDULE 2 – Annex A of the 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:
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
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:
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*
Tratamientos previstos y finalidad	**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:
Consulte *La descripción de la transferencia* adjunta.	*Please refer to the attached "Description of Transfer" document(s)*