Supplier Security Requirements and Expectations

Baseline Requirements for all Suppliers

Supplier Name:
Address:
Respondent Name & Role:

Support Location:
Contact Number:

Supplier Profile:
What is your organizations main business function:
What function(s) does your organization perform for McAfee, LLC:
What is your organizations maturity level in provision of this function:
Is an industry standard accreditation issued by ISO27001, PCI DSS, or independent audit, SSAE-16 or ISAE-3402 audit report or equivalent available?

Signature of responsible party:

	Name:
Role:	Date:
By placing my name in the box above I am acknowledging that I am authorized to agree on behalf of the Supplier named, and do agree to meet the requirements outlined. Any items that are out of scope or that the Supplier cannot meet are identified below.	Yes / No
Areas that are out of scope or that are not met:	

Supplier Instructions:
McAfee's data protection strategy is to perform a due diligence assessment of data protection controls regardless of location. Your assistance to achieve this goal is greatly appreciated. All Suppliers are expected to meet the minimum controls identified in this document. In some cases McAfee requires a written response to this document.

If McAfee requests a written response from your organization you are required to submit an electronic copy of this document confirming compliance. In responding please provide in the space provided above. If there are any requirements that are out of scope or that cannot be complied with, including changes requested by the McAfee Business unit you support, they must be explained in the space provided below the signature box.

Once you have reviewed the completed document please send a copy to the McAfee Business Contact working with you who will work with McAfee Information Risk and Security to complete the assessment process. Please note that if you are handling data that is considered Restricted Secret or above additional reviews will be required as a part of the Supplier review.

1. Security Policy

    a. Supplier must have an Information Security policy in place which meets applicable industry standards and which is subject to review by McAfee under a Non-Disclosure Agreement (NDA). This policy must comply with the laws, regulations, operational procedures and systems security configurations implemented. This policy must be reviewed on a regular basis by the Supplier.
    b. The policy must provide governance for all platforms deployed including mobile computing and Small Form Factor (SFF) devices that require access to McAfee data or McAfee operated systems.

2. Organizing Information Security

    a. Information Security Roles and responsibilities must be clearly defined and implemented.
    b. Non-disclosure agreements must be signed by Suppliers prior to being granted access to McAfee information.
    c. All interactions with McAfee or involving McAfee information must be secured and approved by McAfee.
    d. All subcontracted activities involving McAfee information must be approved and secured by the Supplier.

3. Asset Management

    a. McAfee will generally inform the Supplier of the classification of McAfee data provided to Supplier. In the event Supplier is not certain of the classification of any item of McAfee data, Supplier will seek clarification from its McAfee Business Contact.
    b. An appropriate set of procedures for information labeling and handling must be developed and implemented.
    c. Personal use of McAfee equipment and information is not allowed.

4. Human Resources Security

    a. Security roles and responsibilities of employees, contractors and third party users must be defined and documented to incorporate McAfee's data protection control requirements including background checks to the extent permitted by applicable law.
    b. All employees, contractors, and third-party users must be notified of the consequences for not following your security policy in handling McAfee information classified as confidential and above.
    c. All assets used to manage or store McAfee information must be protected against unauthorized access, disclosure, modification, destruction or interference.
    d. All employees, contractors and third party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.
    e. All personnel with access to personal information (PI) will complete a privacy training class, and be knowledgeable of any specific privacy requirements for the data being handled. Refresh training is required annually.

5. Physical and Environmental Security

    a. Information processing facilities where McAfee confidential and above information is stored must be secured and protected from unauthorized access, damage, and interference.
    b. Physical security must be appropriate to the classification of the assets and information being managed and could include, card key access, security cameras, and solid wall

construction for all exterior walls. Additional controls may be needed for Restricted Secret and Top Secret information or assets.

c. The number of entrances to the information processing facilities in which McAfee Confidential and above information is stored must be limited. Every entrance into these areas requires screening. (e.g. Security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)). Logs must be recorded and maintained.
d. Physical access must be restricted to those with a business need. Access lists must be reviewed and updated at least once per quarter.
e. Process, training and policies must be in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
f. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure. Any alarms must trigger an emergency response.

6. Communications and Operations Management

a. Operating procedures must be documented and managed by a change control process.
b. Supplier must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process.
c. Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.
d. Development, test, and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational system.
e. Acceptance criteria for new information systems, upgrades, and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.
f. Supplier must support standards and procedures that ensure confidentiality, integrity and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.
g. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility.
h. Suppliers must maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. The Supplier must ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response by the third party.
i. Supplier must define the end of life process (EOL) for all websites and applications which could include date of EOL and any business triggers that may result in updated EOL date.
j. Supplier must remove or destroy all Personal Information by the date requested by the McAfee business Contact, or within 30 days of termination of Supplier contract. Copies of data subject to legal data retention requirements or on system backup media that is comingled with other system data are not included. All Restricted Secret or above hard copy data which is no longer required must be shredded by use of a cross cut shredder.
k. All Personal Information transferred must be properly secured. System must not transfer Personal Information to other systems or be used for purposes other than specified, unless approved by McAfee or the individuals the information belongs to. Supplier must inform the McAfee Business Contact of all third parties that the Supplier uses to deliver the service.
l. Access and Accuracy: The system must implement reasonable measures to ensure that the personal information is accurate and current.
m. User Generated Content: all user generated content (i.e. file attachments such as documents, pictures, videos, text, etc.) must be screened for malicious and inappropriate content. Moderation of content must be performed prior to the content being accessible to

other individuals. The McAfee sponsor will provide the Supplier with the moderation criteria.

n. Audit logs recording user activities, exceptions, and information security events must be maintained for an agreed period to assist in future investigations and access control monitoring.

7. Access Control

a. The access control policy must clearly state the rules and rights for each user or group of users including applications and information sharing and must include a process for granting and removing access to all information systems and services. A record of all privileges allocated must be maintained.

b. Each user must have a unique user ID and practice the use of strong passwords which are at least eight characters long and composed of letters, numbers and special characters where feasible. If other biometric controls are used in lieu of passwords or in addition to they must be documented and disclosed in compliance to McAfee Privacy policy.

    i. The use of group IDs is only permitted where necessary and must be approved and documented.

    ii. Suppliers must insure a password is delivered via a secure and reliable method which could include confirming emails to the account holder that do not contain the account name, and a secure temporary password which is changed immediately on login.

    iii. Group and individual accounts should not have administrative access unless absolutely necessary for successful service delivery.

c. Access to applications and data must be reviewed at regular intervals to prevent unauthenticated users from accessing data or using vital system resources and revoked when no longer required.

d. All Client systems must log off after a defined period of inactivity and have password protected screen savers. For laptops and mobile devices increased security access controls (e.g. implement hard disk drive (HDD) password protected access control) must be implemented unless volume encryption or encrypted store is implemented.

e. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, must be disabled or removed.

f. Network segments connected to the Internet must be protected by a firewall which is configured to secure all devices behind it.

g. User connection capability must be documented with regard to messaging, electronic mail, file transfer, interactive access, and application access.

h. All extranet connectivity into McAfee must be through McAfee approved and authorized secure remote connections.

i. All restricted and above data exchanged with McAfee for mission or business critical functions and Business to Business (B2B), require secure intercompany communications (ICC) implemented by McAfee IT Engineering services. The McAfee program manager is responsible for communications funding and will arrange for Suppliers to engage with the McAfee engineering services team.

j. All production servers must be located in a secure, access controlled location.

k. Supplier is responsible for implementing the secure protocols at their sites and managing the protocols by a change control process.

l. Firewall must be configured properly to address all known security concerns.

m. Infrastructure diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution.

n. Systems must have the ability to detect a potential hostile attack. Examples include but are not limited to Network Intrusion Detection (NID) or Host Intrusion Detection (HID) / Prevention. All systems must be updated to current release and actively monitored.
o. Network segments where McAfee data resides should be isolated from non-McAfee data, logically or physically unless approved by McAfee.
p. Access controlled applications must implement a lock out for a minimum of 30 minutes after 5 consecutive failed login attempts and 1 hour after a total of 10 failed login attempts.
    i. Access controlled applications must never be reinitialized by using the back button.
    ii. Access controlled applications that only contain Public data, such as Webinars or virtual tradeshows, may exceed the user lock out after 5 consecutive failed login attempts and must be documented in the response to these requirements.
q. Applications containing Confidential data and above must require a password change every 90 days or less.
r. Applications must never capture and store the user's password and provide it during the login process. A 'reminder' function should only contain the user ID and not the password.
s. All Web applications that allow the input or display of user generated content (including site "Search" parameters) must turn off the Archival flag used by search engines. This prevents the long term archival of web pages that have been compromised or defaced.
t. To prevent all search engines from showing a "Cached" link for McAfee sites place the following tag in the <HEAD> section of every page: <meta name="robots" content="noarchive">
u. Access to source code must be limited and controlled to prevent unauthorized access.
v. Externally facing web applications must logoff unattended sessions at or before 30 minutes of inactivity.
w. Server should have login banners that advise unauthorized access is prohibited.
x. All occurrences of McAfee branded internet hosting are subject to a joint vulnerability assessment led by McAfee Risk and Security Management before going live.
y. McAfee requires daily vulnerability scans performed on all internet facing web sites where McAfee has branded content and is the primary site owner or 'McAfee' is part of the URL. McAfee uses the McAfee vulnerability management solution. Vulnerabilities will be reported to the Supplier for remediation. The Supplier can access the McAfee site for: vulnerability reports, scripts to demonstrate the vulnerabilities and remediation support. McAfee does not charge the Supplier for the McAfee scanning service.
    i. Supplier firewalls must be configured to allow McAfee scanning of McAfee Web applications. McAfee scanning source IP addresses will be provided to Suppliers. ii. If the Supplier currently uses the McAfee vulnerability management solution, McAfee requires access to the reports. Suppliers that use other scanning tools must make scan reports available to McAfee for review.
z. Remediation of vulnerabilities is the responsibility of the Supplier.
aa. Upon identification of security vulnerabilities in a production application, the Supplier must remediate within the approved & agreed time lines
bb. McAfee may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for McAfee compliant plus 'McAfee compliant'.
cc. McAfee considers a web site security compliant when both McAfee plus McAfee security standards are met. Some Medium and Low vulnerabilities have been elevated from the McAfee compliance rating. All vulnerabilities must be remediated to be 'McAfee compliant'. McAfee will notify Suppliers of each of the McAfee security standards not met.
dd. McAfee reserves the right to require an application scan using vulnerability scanning tools as defined in McAfee's contractual development agreement. Supplier or an agreed upon sub-contractor may perform a vulnerability scan of the application and report the results to McAfee and its development staff for review.

ee. Virus scans are required on all uploaded files.
ff. Where the McAfee Local Area Network (LAN) /Wide Area Network (WAN) is resident (McAfee equipment and IP range) and deployed at a Supplier site (outside of a McAfee managed site) the McAfee Network equipment and LAN /WAN must be in a physically secure and in an access managed environment.

8. Information Systems Acquisition, Development and Maintenance

    a. Applications containing or accessing data classified as restricted data must not be hosted on a virtualized system both software and hardware virtualization models
    b. Data that must meet PCI, Sarbanes Oxley Act (SOx), Health Insurance Portability and Accountability Act (HIPAA) or Controlled Technology USA Export Laws are prohibited from being placed on a virtualized system.
    c. All applications should be designed to meet requirements for availability and protected from denial of service attacks.
    d. Application development cycle follows industry accepted Secure Development Lifecycle (SDL) principles, best practices and secure coding best known methods (BKM's).
    e. Systems security patches are installed on production systems on a timely basis according to threat level recommendations of the issuing vendor. Exceptions must be documented and based on defined business process controls.
    f. All applications developed by the Supplier must have a code review prior to being released into the production environment.
    g. Applications that will be hosted within McAfee's environment must be designed to comply with McAfee's minimum security standards for integration with the McAfee infrastructure and are subject to audit and validation by McAfee.
    h. Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. This validation should include establishing a baseline and monitoring traffic for spikes, sources that are out of bounds for target server.
    i. The application must use McAfee provided digital certificates unless approved by McAfee.
    j. If an application is to land within the McAfee demilitarized zone (DMZ) then it must have an appropriate approved architecture for the targeted DMZ landing zone. (Web Interface, application and / or web services and databases
    k. Application security review plan must be submitted if requested for review and approval by McAfee.

9. Information Security Incident Management

    a. A documented information security event management process for Physical and Data security must be implemented which includes incident response, escalation, and remediation.
        i. Information security events and incidents include:
            1. loss of service, equipment or facilities,
            2. system malfunctions or overloads,
            3. human errors,
            4. non-compliances with policies or guidelines,
            5. breaches of physical security arrangements,
            6. uncontrolled system changes,
            7. malfunctions of software or hardware,
            8. access violations,
            9. legal and regulatory violations
            10. Malware

11. Suspicious and benign behaviors that may lead to an event

b. Any security event involving or impacting McAfee and/or a McAfee website must be reported to McAfee. Notification must be within 48 hours from detection if McAfee data, the McAfee brand, logo or trademarks are involved or compromised.
c. Data Retention Logs must be maintained and made available for use in investigations as related to any security incidents.
d. Applications developed by the Supplier will allow all data to be extracted if required by an E-discovery event. The process should allow for data to continue to be extracted until the event is over.
e. Both companies will act in good faith to preserve the other company's evidence and reasonably cooperate with each other and the authorities if needed during an investigation.
f. Each company will be responsible for investigating incidents and taking actions to protect their own interests.

10. Business Continuity (BC) Management

a. Disaster Recovery (DR) plan must be documented and tested annually.
b. All system media has a regularly scheduled backup and restore capability implemented and tested.
c. An application deployed into a cloud environment needs to be developed as a cloud aware app that will include BC/DR mitigations (which could be cloud based)
d. Disaster recovery resources and / or subcontractors must be documented and made available to McAfee upon request.

11. Compliance

a. Supplier must have a process to document non-compliance of any legal, regulatory or privacy instance or control that does not meet local laws and regulations and must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance. The mitigation plan and business decision must be signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability on behalf of the Supplier.
b. Supplier must know and be compliant with all regulatory and local governing laws that are applicable. Examples include but not limited to Privacy, HIPAA, SOx, U.S. Export license, and PCI- digital signature standard (DSS) compliance.
c. Supplier acknowledges that Product (including, without limitation, hardware, software, technical data, servicing, support, and training) is subject to export controls under the laws and regulations of the United States ("U.S.") and any other applicable Governments. Supplier agrees to comply with these laws and regulations governing export, re-export, import, transfer, distribution, and use of Product, and obtain all required U.S. and any other applicable Government authorizations, permits, or licenses.
d. Supplier shall not sell or otherwise transfer Product to any person or entity listed on a denial order published by the U.S. Government or published by any other applicable foreign Governments, irrespective of the country where this person or entity is located, without first obtaining a license or other authorization. Suppliers agrees that neither it nor any of its subsidiaries will export, re-export, transfer, resell, or divert any Product, directly or indirectly, or to provide services using or in support of Product, to any country for which the U.S. Government or any other applicable foreign government requires an export license, without first obtaining the license or approval.
e. Supplier shall not use Product for any purposes prohibited by the U.S. or other applicable foreign Government law, including, without limitation, the development, design, manufacture, or production of nuclear, missile, chemical or biological weapons, unless

authorized by the U.S. Government and other applicable foreign Governments by regulation or specific license. Supplier confirms that Product will not be re-exported or sold to a third party who is known or suspected to be involved in activities including, without limitation, the development, design, manufacture, or production of nuclear, missile, chemical or biological weapons, unless authorized by the U.S. Government and other applicable foreign Governments by regulation or specific license.

f. If Supplier provides servicing, support, or repair of Product, Supplier agrees to conduct servicing in compliance with all export regulations including reporting requirements. Supplier agrees that defense articles, defense services, and technical data subject to control under defense laws and regulations (e.g., the International Traffic in Arms Regulations [ITAR]) must not be transferred to non-U.S. persons, whether located in the U.S. or abroad, without a valid license or agreement approved by the applicable Government authority.

g. Purpose of collection, Notice, and Complaint Management: For applications where an individual enters Confidential Personal Information (phone number, address information, gender) the link to the McAfee Online Privacy Notice Summary (https://www.mcafee.com/us/about/legal/privacy.aspx) must be included on each page where that information is collected, and be easy to find and read by the individual using the application. It is available in many languages. The Notice includes information on how to get in contact with McAfee to submit a complaint. Supplemental information stating the purpose of collection, how it is protected, used and retained should be included in the User Interface, Terms of Use, or in an FAQ document.

h. Purpose of collection, Notice, and Complaint Management: For applications where an individual enters Sensitive Personal Information (banking information, credit card information, government ID, health information, life style preferences) a supplemental privacy notice must exist on each page where that information is collected, and be easy to find, read, and understand by the individual using the application. It must clearly state the purpose of information collection, how it is protected, used and retained. If the User Interface space is limited, this supplemental privacy notice could also be located in the Terms of Use, or in an FAQ document. It must also include the link to the McAfee Online Privacy Notice Summary (https://www.mcafee.com/us/about/legal/privacy.aspx) which is available in many languages. The Notice includes information in how to get in contact with McAfee to submit a complaint.

i. Data minimization: The Supplier may collect no more personal information from individuals than the minimum necessary to achieve the business goal. This business goal must be documented as part of the project, and is available from the McAfee business owner.

j. Choice: Where applicable, individuals must be given the opt-in choice to participate prior to providing their personal information. In addition, individuals should be given the opportunity to stop their participation and request removal of their personal information if they choose to. Exception to this requirement must be approved by the McAfee Privacy Office.

k. Access and Accuracy: Where applicable, the system should have the capability allowing individuals to access, update, or delete their Personal Information when requested. This can be an automated or manual process. The process must be clearly explained to the individual. Exception to this requirement must be approved by the McAfee Privacy Office.

l. Biometrics, Children's information, Unique Identifiers, Logs, Debug info, settings, Central Processing Unit (CPU) utilizations, performance indicators, and any usage data collected from users: Identifiers must not be used. If any of these types of information are in scope for any project, Supplier must contact the McAfee Business Contact to obtain special approval for collecting them. If any of these forms of personal information are in scope for this project, the McAfee business owner must obtain a Privacy assessment for the project.

m. Web Analytics: Web analytics are permitted as long as IP address or Personal Information is not collected. Google analytics is allowed with standard tracking or basic setup. For any other configuration, Supplier must contact the McAfee Business Contact to

obtain a Privacy assessment for the project.

n. Cookies/Tracking: For applications using cookies or other technologies capable of tracking individuals, Supplier must supply the McAfee Business Contact with details on what is collected and technologies that will be used. Supplier must also provide a hyperlink to the McAfee® Cookie Notice at https://www.mcafee.com/us/about/legal/privacy.aspx.
o. Location: Automated mechanisms to obtain individuals' location information must not be used. If this type of information is part of the project scope, you must contact the McAfee business owner to obtain a Privacy assessment for the project.
p. Communications – email/texts: For applications that will use electronic communications, you must adhere to the privacy templates provided by McAfee. Contact the McAfee business owner to gain access to the templates.
q. Remote Control/Access: These types of technologies must not be used. If these types of technologies are part of the project scope, you must contact the McAfee business owner to obtain a Privacy assessment for the project.

12. Virtualization and Cloud Services

a. Data Protection – The geographic location of provider infrastructure resources must be made clear to McAfee. McAfee must be able to control data location in cloud services to ensure compliance with local laws that restrict the cross-border flow of data.
b. Data Protection – Suppliers providing Cloud Service must provide a process for data destruction and secure deletion of any and all McAfee data as needed. This includes a process for sanitization ("zeroing out") of storage containers and removal of ephemeral data.
c. Data Protection – Suppliers providing Cloud Service must have an established method of encrypting sensitive data in storage and in transit following industry best practices.
d. Data Protection – Suppliers providing Cloud Service must securely handle McAfee related data, compute resources, virtual machines resources by providing logical isolation and secure migration.
e. Authentication – Suppliers providing Cloud Service must include methods or options for multi-factor authentication for cloud administrator roles and as required by McAfee tenant business. Furthermore, McAfee expects the Cloud service provider to implement best practices such as Multi-factor authentication for control of access to the service provider's infrastructure management systems.
f. Administration and Access Controls – Suppliers providing Cloud Service must provide McAfee tenants the capability to fully audit McAfee tenant user access and activity within the cloud service. Audit logs must be capable of being exported from the cloud service.
g. Administration and Access Controls – Suppliers providing Cloud Service must limit employee access to the least privilege needed to perform their duties.
h. Policy and Assurance – Suppliers providing Cloud Service must have documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security (examples include ISO27001/2, SSAE16, FEDRAMP, CSA STAR, FIPS 140-2, and Open Data Alliance). McAfee business tenant usage models may drive specific certification requirements.
i. Policy and Assurance – Suppliers providing Cloud Service must demonstrate adherence to Security Development best practices for all code, APIs, and applications deployed and implemented in support of the cloud service.
j. Governance – Suppliers providing Cloud Service must process and advise McAfee of any security breach involving McAfee data or services utilized by McAfee cloud tenants.
k. Availability – Suppliers providing Cloud Service must provide the McAfee tenants with the means to monitor in near real-time service and resource availability

l. Cloud based services must demonstrate how they achieve BC/DR requirements. This can be done within the context of a Cloud service (IE when the cloud service offers capabilities for this).