MSSTAND 1504: Supplier Security Requirements and Expectations (SSRE): For Confidential Data

June 2017

Table of Contents

1 Purpose

The McAfee Supplier Security Requirements & Expectations (SSRE): For Confidential Data establishes uniform standards, authorities, responsibilities, and compliance for third-party McAfee suppliers (Suppliers). This SSRE provides McAfee's expectations for protecting the confidentiality, integrity, & availability of McAfee data and assets. Capitalized terms not defined herein shall have the meaning set forth in Appendix 20 (Definitions and Abbreviations).

2 Target Audience

The audience for this SSRE consists of all Suppliers, and McAfee employees who are responsible for McAfee supply chain management and services. The standard is also applicable to all McAfee end users which include, but are not limited to: employees, contractors, consultants, interns, service providers, partners, vendors, third parties, and entities acting on behalf of McAfee, LLC.

3 Scope

The provisions of this SSRE pertain to all McAfee information systems, and assets. McAfee senior management shall ensure that information systems and assets operated by, or on behalf of McAfee receive adequate security safeguards. This SSRE and the corresponding policies, procedures, and guidelines are intended to (i) identify McAfee security requirements, including workflow, roles and responsibilities, and escalation procedures and (ii) provide oversight to all McAfee systems and assets.

4 Supplier Instructions

This SSRE defines McAfee's minimum security standards for data protection of information classified as McAfee Confidential as well as for all externally developed and/or hosted solutions provided to McAfee. To achieve security compliance, Suppliers and their subcontractors are wholly responsible for implementing all the security controls defined herein to protect the data they manage, host or process for any function or activity implemented on behalf of McAfee.

This SSRE is not intended to be an all-inclusive list of security requirements. Each solution may generate unique or specific requirements that must be addressed with the appropriate security controls and defined in the applicable statement of work executed by the parties.

This SSRE should be reviewed by the Supplier's Chief Information Officer (CIO) or Security Officer responsible for contracted services. It is the responsibility of the primary Supplier to review the SSRE with its subsidiaries and subcontractors responsible for service delivery to McAfee or on behalf of McAfee and to ensure subcontractor's compliance herewith. The Supplier is responsible for conformance to the SSRE when services are performed by itself, its subsidiaries or its subcontractors.

This version of the SSRE covers data classified up to Confidential. The McAfee business owner is responsible for classifying the data of their web application and communicating it to the Supplier. At a minimum, Suppliers must be capable of implementing security controls required to protect data classified as Confidential.

Suppliers shall review all security controls cited in this document and may request clarification where needed. Suppliers shall notify the appropriate McAfee business owner of full compliance in writing authorized by a company official. Existing Suppliers that complied with a previous version of the SSRE must review and adhere to instructions in this document as McAfee may have included important updates/changes from previous versions.

If a Supplier, their subsidiaries, or subcontractors are not fully compliant to all minimum security requirements, the Supplier shall provide in writing the extent of non-compliance and give committed plan of action detailing when the requirements will be fully met. McAfee's Information Security team shall evaluate a Supplier's security capability. If approved by McAfee, the Supplier plans will be documented in the contract. During a contract review, a Supplier's performance of the SSRE security requirements, the completion of non-compliant security controls plus the Supplier's track record for prompt remediation of vulnerabilities will be evaluated.

Suppliers with an industry standard accreditation should submit a copy. Examples include: ISO27001, PCI DSS or SSAE16 - SOC 2 audits performed by an independent auditor in the last year. Suppliers are expected to provide annual updates of the accreditation for the term of the contract.

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

5 Data Classification Definitions

5.1 Security Measures

The McAfee business owner is responsible for identifying the data classification for the solution implemented. For solutions identified as McAfee Confidential or McAfee Restricted, the Supplier must comply with security requirements for both External Facing (Public) and McAfee Confidential or McAfee Restricted data classifications. (Refer to section 13.1 Data Classification and Handling and 13.3 Data Protection Security.) All exceptions must be approved in advance and submitted by the Supplier to the appropriate McAfee business owner.

(a) McAfee Confidential – Information with access limited to those individuals with a business need-to-know. Security requirements apply to all data marked as McAfee Confidential. The Supplier and any of its subsidiaries/subcontractors responsible for contracted services will implement these plus the Public security requirements as a minimum.

(b) McAfee Confidential – Internal Use Only – McAfee Confidential Data that is available to employees and not disclosed to third-parties, unless authorized. Security requirements apply to all data marked as McAfee Confidential – Internal Use Only. The Supplier and any of its subsidiaries/subcontractors responsible for contracted services will implement these plus the Public security requirements as a minimum.
(c) McAfee Restricted – Information with restricted access that is most sensitive and private to McAfee. Requires the highest level of protection from any unauthorized access, disclosure or tampering, whether in hard copy or digital format. Security requirements apply to all data marked as McAfee Restricted. The Supplier and any of its subsidiaries/subcontractors responsible for contracted services will implement these plus the Public security requirements as a minimum.

6 Security Management

6.1 Security Policy

(a) The Supplier must have a security policy in place, which is subject to confirmation by McAfee under a Non-Disclosure Agreement (NDA).
(b) Supplier must reassess and update their security policies on a periodic basis. Changes must be documented and employ change controls.

6.2 Legal and Regulatory Requirements

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

7 Operational Security

7.1 Supplier Management of Systems

(a) Supplier has a specific resource assigned that is accountable for security management.
(b) All systems have malware management which includes up to date signature files running on all production systems.
(c) 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).

7.2 Security Processes

(a) A security incident management process that includes escalations to management, the customer contact and service suspension notices. (refer to section 7.5 Incident Reporting for incidents involving McAfee).
(b) Account management processes are in place to support requests, setup, issuing and closing user and administrator accounts.
(c) Supplier and its hosting provider must have a process to monitor published system vulnerabilities, and to remediate them within the manufacturer's guidelines for the threat level.

(d) Supplier and its hosting provider must have a process and resources assigned to remediate system vulnerabilities identified by the McAfee vulnerability management scan in the response time specified in Section 14.4 Vulnerability Management.
(e) Suppliers that use subcontracted services are required to have the SSRE reviewed by all subcontractors. Any security measures that are non-conforming by any subsidiary or subcontractor are the responsibility of the Supplier.

7.3 Separation of Duties

Supplier must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process.

7.4 Training and Awareness

(a) Supplier personnel must be trained in Supplier security policies and be required to know changes or updates to these policies.
(b) Security training, including new threats and vulnerabilities, is required for all developers and system administration staff.
(c) All personnel with access to confidential data will have information security training for their respective roles.
(d) All personnel receive regular updates to their training for their respective roles.
(e) All personnel with access to Personal Information (PI) 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.
(f) 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.

7.5 Incident Reporting

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. (Also refer to Section 8.1 and 9.1 regarding cooperative security investigations and the preservation of system logs)

8 Physical Security

8.1 Access Control

(a) Every entrance into the Supplier's data center requires access control (e.g. security guard, badge reader, electronic lock, a monitored CCTV). Logs should be recorded and maintained for 90 days.
(b) Physical access should be restricted to those with a business need and employee access is restricted to the minimum necessary to perform the job. Access lists should be reviewed and scrubbed at least once per quarter.
(c) Supplier facility should have 24x7 intrusion detection.
(d) All controlled area emergency exit doors should sound an alarm when opened. All doors should have automatic closing devices.

(e) Termination of any employee with access to system data must have their accounts disabled immediately.

8.2 Telecommunications Security

(a) All telecommunications equipment must be located in a secure room with managed access control.
(b) All equipment must have the installation or default passwords removed.

9 System Security

9.1 Logging of Security Events

(a) Any security event where a McAfee website had unauthorized access or was compromised must be reported to McAfee. See section 7.5 on Incident Reporting.
(b) All systems and applications must be designed to log, monitor and report all security events. Logs must be tamper proof and/or off system write only log files.
(c) In the event of an incident, audit trails must be available to assist investigations. McAfee may request to cooperatively work with the Supplier on security forensics for some incidents.

9.2 System Access Control

(a) System Administrators must have a separate admin account for performing administration tasks.
(b) Only authorized users are permitted to gain access, via secure authentication processes. Access controls must limit access based on business need, following the principle of least privilege and ensuring individual accountability.
(c) System account sharing is prohibited.
(d) Internet facing accounts must use secured authentication. System authentication must be authorized at run time via secure web based authentication methods.
(e) Account creation or collection of personal information must be encrypted via TLS 1.1 or higher, or SSH certificates signed by an externally trusted Certificate Authority (CA).
(f) Access must be enforceable to the granularity of individual users. Users must have a unique user ID.
(g) User roles within the application must be based on business need and determine the level of access a person requires (e.g. editor – read/write/delete, reviewer – read-only)

9.2.1 Password and Password Reset Processes

(a) Passwords must be at least eight characters long and be composed of letters, numbers and special characters.
(b) There is a secure and reliable method of processing and delivering a reset password.
(c) The password reset process has controls that ensure only the authorized user can request a password reset. The reset process verifies the account holder by sending a confirming e-mail. Any password communication will not contain the account name for the logon.
(d) Access controlled applications must never be reinitialized by using the Back button of a browser.

(e) Access controlled web application session time outs must discontinue after 30 minutes or less of inactivity. (Exceptions for Webinars or virtual tradeshow applications must be documented as a Supplier response to the SSRE).
(f) Access controlled applications containing Confidential Data 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.
(g) 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.
(h) Applications must require a password change every 90 days or less.
(i) Password history must be enforced by preventing the use of the previous 24 passwords.

10 Server Security

(a) All production servers must be located in a secure, access controlled location.
(b) All systems must be hardened prior to production use including patching of known vulnerabilities. Disable all generic, guest, maintenance and default accounts.
(c) 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.
(d) Test accounts and user accounts are removed/revoked when no longer required.
(e) Development and test systems are isolated from production environment and network.
(f) Disable all non-required ports and/or services on server operating systems and firewalls.
(g) Consoles with keyboards have password protected screen savers that logoff unattended.

10.1 Intrusion Detection

(a) 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.
(b) 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.

10.2 Virtualized System

(a) Any single image of data classified as Confidential defines the minimum security requirement for all virtual instances on the same host system.
(b) Virtualized systems may contain data classified as confidential data.
(c) Applications that require physical separation cannot be on the same host system.

10.3 Cloud Services and Systems

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

(e) Any changes to the architecture or function of a service or data model in the cloud must first be reviewed and approved by McAfee.
(f) Applications that require physical separation cannot be on a cloud based service.
(g) 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.

11 Network & Client Security

11.1 Remote Access

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

11.2 Client Security

(a) 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.
(b) Clients must have Malware protection with automatic signature updates.
(c) Systems located in an unsecured area and attached to the Supplier network must not access systems and network segments containing confidential data.
(d) All client systems that access confidential data, whether in use or not, must be physically secured. (Refer to section 13.3.2 Data on Portable Systems and Devices for portable system requirements.)
(e) 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.

12 Firewall Setup

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

13 Data Security

13.1 Data Classification and Handling

(a) Appropriate security measures must be in place to address data handling, access requirements, data storage and communications (in transit).

(b) McAfee Confidential – Need-to-know access and must have a data audit trail. Secure authentication and authorization is required. Secure encrypted communication is required.
(c) McAfee Confidential – Internal Use Only – McAfee employee access only unless authorized. Must have a data audit trail. Secure authentication and authorization is required. Secure encrypted communication is required.
(d) McAfee Restricted – Must be monitored with controlled access at all times. Must have a data audit trail. Secure authentication and authorization is required. Secure encrypted storage and communication is required.

13.2 Privacy Management

(a) Applications such as "Software as a Service' used by McAfee to collect Personal Information must have the URL for the McAfee Privacy Statement embedded into the web page where PII is collected. It is available in all languages.
(b) Where applicable, individuals must be given the opt-in choice to participate prior to providing their Personal Information. Opt-in selection boxes are not pre-selected by default.
(c) 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.
(d) System must not transfer Personal Information to other systems or be used for purposes other than specified.
(e) System must have appropriate security controls to avoid unauthorized access, disclosure and / or use or modification of individuals' Personal Information.
(f) The system must adhere to the Federal Trade Commission's CAN-SPAM Act if it:
    - Requests input of Personal Information from an individual to complete "Email to a Friend" notifications, or
    - The system offers online, subscription based communication services.

13.3 Data Protection Security

(a) Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their subcontractors.
(b) For data classified as McAfee Confidential, McAfee Confidential – Internal Use Only or McAfee Restricted, data should be encrypted using AES-128 or stronger.
(c) To protect data Integrity, data should be hashed using SHA-256 or stronger.
(d) All Confidential hard copy data that is no longer required must be shredded by use of a cross cut shredder.

13.3.1 Print Controls

The print process must be adequately secured to prevent unauthorized disclosure/access.

13.3.2 Data on Portable Systems and Devices

(a) 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.

(b) Portable systems with confidential data must not transfer data by use of Personal Area Networks.

13.4 Data Backup, Retention and Disposal

(a) Web sites and applications must be backed up in accordance with Business Continuity and Disaster Recovery requirements specified in section 16 Business Continuity and Disaster Recovery.
(b) Supplier must secure all backup media during transportation and in storage.
(c) 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.
(d) 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.
(e) 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.

14 General Requirements

14.1 Application Development

14.1.1 General Best Practices:

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

14.1.2 Security Reviews:

(a) Web application vulnerability assessments must be performed during the application development and the deployment lifecycle. (Refer to section 11.5 Vulnerability Management.)

(b) All 3rd party software included in the application must meet all security requirements outlined herein.
(c) Secure interfaces for USER LOGIN and user data input of Personal Information must utilize certificates signed by a trusted Certificate Authority (CA) only. Examples: HTTPS / TLS / SSH.

14.2 Security of System Files

(a) Access to source code must be limited and controlled.
(b) During and after development, all applications must ensure the security of system files, plus access to source code and test data.
(c) All back-door maintenance hooks must be removed from the application before production use.
(d) Application architecture must prohibit databases containing confidential information from residing on the same server as the application.
(e) 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).

14.3 Application Availability

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

14.4 Vulnerability Management

(a) McAfee requires daily vulnerability scans performed on all internet facing web sites where McAfee has branded content and is the primary site owner or 'McAfee' is part of the URL. McAfee uses the McAfee Secure vulnerability scanning solution. Vulnerabilities will be reported to the Supplier for remediation. The Supplier can request information for: vulnerability reports, demonstration of the vulnerabilities (when available) and remediation support. McAfee does not charge the Supplier for the McAfee Secure scanning service.
(b) McAfee requires daily access to the reports.
(c) Upon identification of security vulnerabilities in a production application, the Supplier must remediate within the following time lines:
    - Urgent or Critical, McAfee threat rating [5] or [4] must be remediated in 1 to 5 calendar days.
    - High, McAfee threat rating [3] must be remediated within 10 calendar days.
    - Medium, McAfee threat rating [2] must be remediated within 30 calendar days.
(d) If the security vulnerabilities identified by the McAfee vulnerability scanning process have not been addressed in the above timelines, McAfee may shut down the web site until the vulnerabilities are remediated. Returning the site to production status requires the site to pass a scan for McAfee compliance. (See 5)
(e) McAfee considers a web site compliant when McAfee security standards are met. McAfee Security will notify Suppliers of each of the McAfee security standards not met.

14.4.1 Input Moderation of User Generated Content (UGC)

(a) All sites that allow input or display of user generated content (file uploads, usually rich media or text input) and content that is rebroadcast to mailing lists of other users, must be moderated. Moderation of rich media must be by McAfee personnel or contracted service agents who are trained for the task. Moderation of text can be via automated tools. Automated moderation tools should include the word “porn” in the search.
(b) All site users inputting UGC are required to be registered and authenticated by a password. Anonymous posting of UGC is not allowed without full moderation. This includes site registration by use of e-mail address without confirmation since there is no validation of the user.
(c) All UGC must be logged to the user and time stamped.
(d) All sites accepting UGC must contain links to:
- McAfee’s Terms of Use
- McAfee’s Terms of Service with proactive acceptance of terms (this occurs during user registration)
- McAfee’s Digital Millennium Content Act (DMCA) Notice and Procedure

(e) Under certain circumstances community monitoring may take the place of moderation. This must be reviewed and approved by McAfee’s Information Security team as an exception to these requirements. If this exception is approved, the following minimum controls will be required:
- Only text comments (no anonymous blogging, rich media, or embedded links allowed).
- Must have automated validation to block inappropriate, Bot created or malicious text from being posted.
- Web forms must have input validation to ensure input is encoded as text only.
- Must have flagging capability so other users can escalate inappropriate comments.
- Must have a monitoring process (after the fact) performed by McAfee or McAfee representatives with the appropriate training.

(f) Virus scans are required on all uploaded files.
(g) All URL’s & JAVA Script, RSS, Twitter feeds and widget content input to a web site is scanned for viruses and moderated by automated tools.

14.4.2 Removal of Search Engine Archival Flag

(a) No search engine archiving of new, revised or updated Web sites containing user generated content.
(b) All new 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.
(c) 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">

15 Extranet Requirements

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

16 Business Continuity and Disaster Recovery

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

17 Deviation from Use

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

18 Duration

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

19 Cross References

- **MSPOL 1400 Access Control Policy**
- **MSPOL 1500 Data Ownership, Classification and Handling Policy**
- **MSPOL 1600 InfoSys Acquisition, Development and Maintenance Policy**
- **MSPOL 1700 Communications and Operations Policy**

20 Definitions and Abbreviations

Application Security:	Refers to protecting data processed by an application, as well as the integrity and availability of services provided by the application.
Business Critical:	Loss that indirectly impacts a Mission Critical function, or directly impacts a business unit's primary function is considered Business Critical.

Cloud Computing:	Computing resources, software and data delivered as a hosted service over the Internet. The computing resources are dynamically scalable and often virtualized. The services are accessible anywhere that provides access to networking infrastructure.
Content Moderation:	A business process where content is reviewed and approved by McAfee or a McAfee representative with the appropriate training before it is viewable by others.
Content Monitoring:	A business process where content is reviewed (and removed if necessary) by McAfee or a McAfee representative with the appropriate training after it is viewable by others.
External Facing (Public):	Information available without approval or authentication.
Confidential Data:	Information with restricted access limited to those individuals with a need to know.
Mission Critical:	Loss that directly impacts McAfee's ability to Book, Build, Ship, Order, Pay, Close or Communicate is considered Mission Critical.
Moderation:	A business process where McAfee personnel or a contracted agent reviews and either approves or rejects user generated content (UGC) based on the business situation. Automated moderation is when computerized searches are performed on UGC to screen the input for unwanted or malicious input. Community moderation for appropriateness of content is reporting by the user community of violations of content after it is posted.
Physical Security:	Measures taken to protect systems, buildings and related support infrastructure against threats from the physical environment.
Personal Information (PI):	Any information that can be used to identify, contact or locate someone, plus any other information associated with it.
Privacy:	An individual's right to have a private life, to be left alone and to be able to decide when their personal information is collected, used or disclosed.

User Generated Content (UGC):	Content input into a web application either by text input or rich media such as pictures, audio and videos via file uploads or widgets.
Unsecured Area:	Areas that are not controlled by physical access security measures. Some examples are: the lobby of an access controlled building or a warehouse delivery dock with PC access to corporate systems.
Virtualized System:	The use of the term ‘virtualized system’ includes any of the following: A virtual machine (VM) is a software implementation of a computer that executes programs like a real machine. The virtual machine monitor (VMM) or hypervisor is the software layer providing the virtualization. Platform virtualization and /or hardware virtual machines that allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. Also included are other "virtual environments" (also called "virtual clients” and “virtual servers") that provide some form of encapsulation of

21 Revision History

Document Preparer			
Name	**Designation/Role**	**Email Address**	**Date**
Bruce Weed	GRC, Information Security	bruce_weed@mcafee.com	June 2017
Document Classification History			
Classification	**Restrictive Markings**	**Change Description**	**Date**
McAfee Confidential	McAfee Confidential	Default classification for most company generated documents.	June 2017

Document Revision History			
Name	**Version**	**Change Description**	**Date**
Bruce Weed	1.0	Publish initial version.	June 2017

22 Approvals

Role	**Stakeholders (Title)**
Standards Owner	Grant Bourzikas
Standards Author	Bruce Weed
Standards Contributors	Michelle Greer, Frank Haran, Bruce Weed, Nicole Robinson
Standards Reviewers	Michelle Greer, Bruce Weed, Eric Bowerman, Nicole Robinson, Tiffany Lim, Keysha Council
Standards Approvers	Tony Gunn

23 Appendix

No appendices at this time.