McAfee Enterprise Information Security Overview

2019
# OVERVIEW

## Table of Contents

3   The McAfee Pledge  
4   Introduction  
4   Office of the Chief Information Security Officer (OCISO)  
5   Information Security Management System  
5   Information Security Risk Management  
6   Security Is Everyone’s Responsibility  
6   Working on a Secure Network  
7   Cloud Security  
7   Data Protection  
8   Lawful Transfer of Personal Data  
8   Developing Secure Products  
9   Maintaining Availability  
9   McAfee Cybersecurity Fusion Center  
9   Incident Response  
9   Reporting  
9   Learn More
The McAfee Pledge

We are McAfee.

We make the world a safer place. This is our pledge. Our cybersecurity expertise is foundational to how the world views McAfee. The outcomes we drive matter. That’s why each and every day we use our talent to create technology that safeguards human progress. We consistently, reliably, and effectively protect all that matters through leading-edge cybersecurity, from the workplace to the home and everywhere in between. But we are known for more than what we do. We also are revered for who we are. Our integrity informs every action we take and every word we speak. You are the reason our brand is trusted to protect companies large and small, as well as organizations and governments around the globe, not to mention hundreds of millions of people connected through the transformational power of technology.

How we do business defines us. That’s why we steadfastly draw on our courage to fight cybercrime, even as our adversaries relentlessly turn the promise of technology against all of humanity. We gladly collaborate with competitors for the higher good. And we partner with the U.S. government, national agencies, and international law enforcement to ensure our deep knowledge and compelling innovations have the greatest impact in efforts to defend our country and the free world.

How we treat one another and our stakeholders—from customers and partners to suppliers and the communities where we work and live—is characterized by our core values. That’s why each of us is responsible for living our Code of Conduct, which includes deliberate and full compliance with the letter and spirit of the law as well as ethical behavior. Our Code of Conduct ensures that our values inform every project, every team, every office, and every relationship that we earn around the world. Not only do we make the world a safer place, but by making a personal pledge to act honestly, ethically, and with full diligence in support of our Code of Conduct, we also make the world a better place.

Chris Young CEO, McAfee
Introduction
This document provides an overview of the McAfee® Enterprise Information Security Program.

Office of the Chief Information Security Officer (OCISO)
Information security is at the core of McAfee and has the full support and commitment from our CEO and top executives.

McAfee has implemented a centralized, global information security program led by the Office of the Chief Information Security Officer (OCISO). The OCISO organization is comprised of five main sub-organizations to support the confidentiality, integrity, and availability of McAfee information, assets, products and services, and those that are entrusted to us. Those sub-organizations are:

- Governance and Assurance
- Security Architecture
- Security Engineering: Device, Network and Cloud
- Security Intelligence: Fusion Center, Physical Security, and Industrial Security
- Product Security and Vulnerability Management

The OCISO organization is customer zero at McAfee. We use our own McAfee products throughout the enterprise to prevent, detect, and respond to cyberthreats that affect our business. By operating as customer zero, we are able to provide our product management teams valuable feedback which helps to ensure that the McAfee products we deliver to our customers are best in class.

With CEO and top executive commitment to information security and a global CISO-led security organization, McAfee engages, trains, and expects the entire workforce to exercise security in their daily role, as security is everyone’s responsibility.
OVERVIEW

Information Security Management System

The McAfee® Information Security Management System (McAfee ISMS) is at the core of the global information security program. It is designed to ensure that a risk-based approach is taken for the selection, implementation, and monitoring of appropriate security controls throughout the organization.

The baseline security controls that comprise the McAfee ISMS are based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 4 and are further derived into management, operational, and technical categories. Industry standards, best practices, and additional security control frameworks may be used for specific zones and products beyond the McAfee baseline, such as Payment Card Industry Data Security Standards (PCI DSS), FedRAMP, ITGC/SOX, and others.

A set of internal policies and procedures govern the implementation, monitoring, and effectiveness of the security controls.

Governance of the McAfee ISMS is maintained by management system reviews and operational reviews, focused on security operational control monitoring.

The McAfee ISMS aligns and is certified to ISO/IEC 27001:2013.

Information Security Risk Management

As part of the McAfee ISMS, McAfee® Information Security Risk Management (McAfee ISRM) is critical for ongoing identification of threats, vulnerabilities and risks to the enterprise.

The McAfee ISRM consists of three tiers:

Each tier comprises of four phases to complete the McAfee ISRM process:

Each tier of the McAfee ISRM is built into existing business processes to provide continuous identification and management of risks. Information security risks are captured into a risk register and reported. McAfee ISRM provides input into the McAfee ISMS baseline security controls.
OVERVIEW

Security Is Everyone’s Responsibility
The high level of security at McAfee relies on a well-trained workforce.

Where permitted under applicable law, McAfee employees are screened prior to hire, including undergoing and passing background checks. McAfee personnel are required to acknowledge and consent to McAfee security and privacy policies once onboarded, including confidentiality obligations.

Once onboarded, McAfee personnel receive annual security awareness and data protection training as well as more detailed, role-based training where appropriate.

In addition to training, ongoing security awareness activities based on identified risks and best practice are conducted throughout the year, such as the McAfee® Immersive Phishing Program. As part of this program, McAfee personnel receive, at a minimum, one monthly simulated phishing email. Those who fall susceptible receive targeted training focused on identifying and reporting phishes.

Working on a Secure Network
The McAfee network is based on a segmented architecture, where certain zones are authorized for certain types of data processing, which then correspond to specific security controls.

Change management and security management enable McAfee to stay up to date on patches using centrally managed tools for deployment. In addition, production changes are run through the McAfee® Change Advisory Board (McAfee CAB) for documentation and approval as necessary.

Computer systems on the McAfee networks and computer systems used for McAfee business purposes have current, approved security and malware protection measures in place. McAfee implements malware protection at a variety of locations, including, but not limited to the network, data centers, endpoints, servers, and email infrastructure. Logical access means are tested to determine their resistance to attacks and help to avoid any degradation or unwanted deletion.

McAfee performs vulnerability scanning monthly, at a minimum, against the internal infrastructure and at a minimum weekly externally to help ensure the latest content operating system and application level updates are applied.

Attack and penetration (A&P) testing is generally performed annually and performed quarterly in certain zones with critical data (such as the PCI zone) on existing services. New services are tested prior to production implementation. A&P testing is conducted using a combination of internal McAfee resources and external service providers.
Remediation of vulnerability scans and A&P is prioritized based on the severity of the vulnerability.

Third parties are not granted access to internal McAfee systems without appropriate contractual agreements and security processes in place to appropriately protect McAfee data and assets.

Mobile devices connected to the McAfee network and information are required to be managed, helping to ensure that our mobile security controls are implemented and monitored. Additionally, mobile devices are not allowed to connect to our segmented production environments where customer data may be stored, processed, or transmitted. It is against company policy for McAfee information to be transferred or otherwise copied to a non-managed application or service.

**Cloud Security**

McAfee understands that cloud data security is critical. The security team works closely with our IT, engineering, and legal teams to understand and implement the required security controls for the relevant frameworks associated with cloud computing.

Cloud management plane access is restricted following identity and access management (IAM) best practices, including utilizing multifactor authentication (MFA).

Asset discovery tools are implemented, and relevant data security technologies are used to protect McAfee information, including that of our customers, in McAfee controlled environments. Technologies implemented include data loss prevention (DLP) and encryption (client-side and server-side), as well as obfuscation, anonymization, tokenization, and masking. Continuous auditing occurs to highlight and help prevent possible data exposures.

External-based perimeter assessments are performed at least weekly to significantly limit the attack vector and reduce the attack surface.

**Data Protection**

Data protection is a high priority for McAfee. Regardless of whether data is processed (collected, used, retained, disclosed, disposed, or otherwise acted on) on the McAfee network, on a third-party vetted and approved cloud network, or on a “bring your own device,” security controls are in place that are designed to ensure protection.

McAfee requires the use of appropriate cryptographic controls to protect personal data—also known as personally identifiable information (PII) and personal information—in transit and at rest on removable media. This includes hard disk encryption on endpoints, including laptops.
OVERVIEW

McAfee data protection policies are designed so that access to all information assets is granted in a controlled manner based on the requester’s “need-to-know,” subject to the approval of the designated information asset owner and consistent with the “least privilege” principle.

Lawful Transfer of Personal Data
McAfee has executed internal IntraGroup Agreements for lawful transfer of personal data by McAfee and has submitted Controller and Processor Binding Corporate Rules applications, with Ireland as the lead regulator. The McAfee® MVISION Cloud products (formerly Skyhigh Networks) have self-certified compliance with the Privacy Shield Framework. McAfee offers a Data Processing Agreement for customers upon their request.

Developing Secure Products
McAfee applications, whether purchased or developed internally, are subject to a release-to-production security review process.

McAfee product software, IT applications, and cloud services are designed for security and privacy (using Security and Privacy by Design principles), while rigorous procedures are in place to find and remove security defects throughout the software lifecycle. These procedures define the McAfee® Security Development Lifecycle (McAfee SDL), which consists of 32 technical, operational, and enterprise-level activities and reinforce our commitment to building secure software.


A subset of our McAfee products has obtained independent third-party validation through SOC 2 Type II Accreditation, FedRAMP Authorization, and others. Please visit the McAfee® Trust site to review security compliance certifications for specific McAfee products: [trust.mcafee.com](http://trust.mcafee.com).

McAfee Public Sector (FIPS 140-2, 186 and Common Criteria Validation):
OVERVIEW

Maintaining Availability

McAfee recognizes that business continuity management and disaster recovery are holistic management processes and maintains a comprehensive corporate framework addressing continuity of operations that includes emergency response, crisis management, business continuity, and disaster recovery.

McAfee has business continuity plans with respect to significant business disruptions of critical operations. Such plans are structured to redirect and support McAfee and its customers in the event of an unexpected, harmful, or destructive incident. Core business services are replicated across McAfee offices and data centers. Should one site fail, services are redirected to other sites.

McAfee leverages, among other practices, the following business continuity strategies:

- Relocating impacted businesses to designated recovery locations
- Using redundant processing capacity at other locations
- Rehearsing and testing recovery procedures

McAfee Cybersecurity Fusion Center

The McAfee® Cybersecurity Fusion Center is where physical security and cybersecurity converge. Merging logical and physical security in the state-of-the-art McAfee Cybersecurity Fusion Center helps to ensure that all types of events, incidents, and cyberattacks are detected and responded to in a timely manner.

The McAfee Cybersecurity Fusion Center’s operations team identifies, hunts for, and react to threats. The tools used for these activities consist primarily of McAfee products supporting the customer zero concept.

McAfee facilities utilize cameras and locks/key card/badge access, which are monitored in its physical security practice. The McAfee Cybersecurity Fusion Center is physically and logically geo-redundant to maintain continuity.

Incident Response

McAfee maintains multiple information security incident response teams that follow established procedures for incident response training, testing, handling, monitoring, reporting, and response assistance. These procedures help control and minimize the impact of an information security incident by defining the appropriate team and process by which to report and address an incident.

Reporting

The OCISO organization holds weekly operational reviews focused on security operations metrics, such as number of incidents, time to detect, and time to respond. This is part of overall McAfee ISMS governance.

Learn More

To learn more about McAfee security practices in our business and in our products, please visit the McAfee® Trust site: trust.mcafee.com.
About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies’ products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.