Information Security Best Practices

This Manual includes Freddie Mac's suggested tips and best practices to assist Multifamily Seller/Servicers and its vendors in understanding and following the information security requirements in Section 2.26 of the Freddie Mac *Multifamily Seller/Servicer Guide* (Guide). Please note that this Manual does not supersede or replace any applicable laws or regulations or the Seller/Servicers' own legal practices and procedures regarding compliance with the information security requirements in the Guide, but instead provides guidance and tips on how Seller/Servicers can support these Guide requirements more effectively. The Seller/Servicer is solely responsible for adopting and maintaining information security measures that are consistent with the information security risk associated with conducting business with Freddie Mac, including any information security measures that exceed the minimum information security standards established by Freddie Mac in Section 2.26 and the guidance and tips provided in this Manual.

References to any products, services, or vendors do not constitute an endorsement or imply a recommendation by Freddie Mac. Each Seller/Servicer must perform its own due diligence and make its own business decision regarding which product, service, or vendor best meets its needs.

Please reach out to the Counterparty Data Security Team at MF_Data_Security_and_Privacy@FreddieMac.com with any questions regarding this Manual.

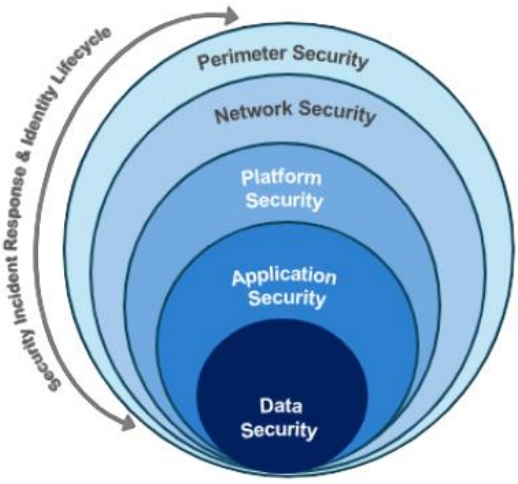
This Manual contains best practices on the following:

- Information Security Program
- Access Management
- Incident Notification to Freddie Mac
- Other Best Practices

Information Security Program

Defense in Depth Approach

Apply a defense in depth approach, which assumes that any control may fail and provides redundancy to eliminate single points of failure.



Objective
"Stop attackers at the gate"
"Keep traffic where it belongs, preventing lateral movement and aids in detecting irregular activity"
"Maintains system standards, configuration integrity, and manage privileged access"
"Protect applications by reducing application vulnerabilities and securing system boundaries"
"Prevent data loss, inappropriate access and ensure recoverability of backups"
Security Incident Response: "Detect and respond to suspicious behavior at all layers"
Identity Lifecycle: "Provide identity and access services to all layers"

Human Resources Security

Management should maintain an acceptable use policy, and employees should be required to acknowledge or agree to it in writing. Elements of an acceptable use policy include:

- Specific access devices that can be used to access the network
- Hardware and software changes the user can make to their access device
- Purpose and scope of network activity
- Permitted network services
- Information than can or cannot be transmitted, and authorized transmission methods
- Bans on attempts to break into accounts, crack passwords, or disrupt service
- Responsibilities for secure operation
- Consequences of non-compliance

Training for personnel should support security awareness and strengthen compliance with security and acceptable use policies. Training materials should focus on:

- End-point security
- Log-in requirements
- Password administration guidelines
- Phishing and social engineering attempts
- Loss of data through e-mail and removable media
- Unintentional posting of confidential or proprietary information on social media

Training materials should be reevaluated as the risk environment changes.

A thorough background check should be conducted for all candidates prior to employment or contractor status for any individual that will have access to Freddie Mac information.

Physical and Environmental Security

Develop, approve and maintain a list of personnel with authorized access to facilities where information systems reside, including an access privilege review performed at least annually and upon departure of authorized personnel.

Physical security controls include:

- Access cards/ID checks
- Physical penetration testing to test perimeter defenses and security controls

Additionally, store data at rest at a secure, off-site facility.

Removable Media Controls

To avoid the risk of data exfiltration and malware ingestion, disable or restrict the use of removable media devices such as USB ports, CD drives, memory card ports, and similar storage devices that can be used to connect an unauthorized device.

Anti-Virus Program/Updates

Utilize antivirus software (*e.g.*, McAfee, Norton, Bitdefender, Malwarebytes, etc.) to detect and prevent attacks from malicious software and keep all such software up-to-date with the latest anti-virus software definitions.

Network Controls

Tools which protect networks by enforcing and detecting perimeter protection include:

- **Virtual Protection Networks (VPN)** enable two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between endpoints.
- **Firewall** is a network security device which acts as a gateway to monitor and filter incoming and outgoing network traffic. A **stateful firewall** is a firewall inspection technique that examines the claimed purpose of a communication for validity. For example, a communication claiming to respond to a request is compared to a table of outstanding requests.
- Utilize up-to-date **Data Loss Prevention (DLP) software** and a corresponding management process to identify, monitor and protect confidential data wherever it is stored, used or in transit over the network and at the perimeter.
- **Intrusion Detection System (IDS)** tools monitor network traffic for suspicious activity and issues alerts when activity is discovered. **Intrusion Prevention System (IPS)** tools combine the analysis functionality of IDS with the ability to intervene and prevent the bad traffic from interacting with the network.

- **Proxy Servers**, such as Zscaler, direct all web traffic to only whitelisted websites and monitors all traffic, including encrypted traffic. Proxy servers act as a gateway to prevent attackers from entering a private network.
- **User Behavior Analytics (UBA)** tools monitor networks for abnormal user behavior and generate alerts for insider threats.

Mobile Computing

Use **Mobile Device Management (MDM)** software to secure and enforce corporate policies on laptops, smartphones, tablets and other mobile endpoints. Common MDM features include enforcement of enterprise password standards, remote wipes, data protection using partition and encryption, asset inventory and tracking and app management using an enterprise app store.

Some other general best practices related to mobile device usage include:

- Keep software/applications up to date
- Keep Bluetooth off when not in use
- Avoid connecting to public Wi-fi networks
- Use a strong lock-screen password and/or biometric authentication
- Do not use public USB charging stations and use only original charging cords or accessories purchased from a trusted manufacturer
- Disable location services when not needed

Vulnerability Management

Vulnerability Management involves the identification and testing of known software vulnerabilities of a system and the prioritization of remediation according to likelihood of occurrence and impact of exploitation.

Penetration testing, or ethical hacking, is the authorized process of identifying security weaknesses to gain access to systems while mimicking actions of potential hackers. “White hat” hackers are professional penetration testers who can assist companies by conducting penetration testing on systems.

Employ a qualified and independent third party to conduct penetration testing on system or system components at least annually. Maintain a record of identified vulnerabilities, their prioritization and a plan for remediation.

Vulnerability testing tools include:

- **Vulnerability scanners –** A vulnerability scanner detects network and web application vulnerabilities. Examples include Nessus Tenable, OpenVAS, Tripwire and Rapid7.
- **Metasploit –** An exploitation framework with a package of products with various capabilities. Using Metasploit and coding skills, an ethical hacker can generate malware and shellcode, gain access, and perform privilege escalation attacks.
- **Burp suite –** A tool used for testing web applications to detect vulnerabilities to exploit.

- **DirBuster –** A multi-threaded Java application designed to brute force directories and file names on web/application servers.
- **Kali Linux –** Advanced Penetration Testing Linux distribution used for penetration testing, ethical hacking, and network security assessments.
- **Core Impact –** A software that provides a comprehensive framework to perform penetration tests within a controlled environment.
- **Static application security testing (SAST) –** A tool that reviews the source code of software to identity sources of vulnerabilities.

Configuration and patch management

Configuration management is the process of maintaining computer systems, servers and software in a desired, consistent state. Configuration management establishes security baseline standards and involves 'hardening' the hosts, servers and network components. An environment can be hardened by:

- Reducing functionality and features to the minimum required
- Opening only necessary logical network ports required to support business function
- Removing all unwanted applications and whitelisting allowed applications
- Applying hardened configuration settings to reduce the attack surface
- Creating hardened OS images and using the image while building new systems
- Patching the operation system and all applications
- Continuously monitoring Baseline Security Configurations (BSC)

A **Configuration Management Database (CMDB)** contains all relevant information about the hardware and software components used in an organization

Patch management is the process of maintaining computer networks by performing regular patch deployments. There are three types of patches:

- **Security patches –** Patches created when a security vulnerability is identified. A security patch should be installed immediately after it is released as hackers will begin to hunt for the vulnerability.
- **Bug fixing patches –** Patches created to fix application errors.
- **Performance and feature patches –** Patches for general updates to software to improve operation, computing speed and user experience

Patches and software updates should be applied to a test environment before deployment. It's recommended to use automated patch deployment software to deploy patches across an enterprise. Some commonly used tools include:

- Microsoft System Center Configuration Manager (SCCM)
- Windows Server Update Service (WSUS)
- ManageEngine
- Ivanti
- Automox
- Red Hat Satellite

Audit logs

Audit logs are records of all system activities tracked using a variety of tools and used to identify unauthorized access or changes made to a monitored system.

Security Information and Event Monitoring tools (*e.g.*, Splunk) gather data from various systems and assess application performance, identify issues and detect attacks before they affect services.

Logs from the following tools or systems should be collected and audited periodically:

- Routers and firewall logs
- Intrusion detection or Intrusion prevention systems
- Remote access logs (*i.e.*, VPN logs)
- Proxy server logs
- Authentication server and password change logs
- Antivirus and malware detection service logs
- Client request and server response
- System availability and usage information
- System events and alerts
- System access records
- Application logs

System Development Life Cycle (SDLC) process

The SDLC is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal. Information security must be integrated into the SBLC to ensure appropriate protection for the information and that the system is intended to transmit, process and store.

More information about the SDLC can be found in the National Institute of Standards and Technology (NIST) Information Security Handbook.

Data Encryption

Encryption is the process of encoding or obfuscating communications and data storage, particularly authentication and transmission of sensitive information.

Data is encrypted differently throughout the following three phases:

- **Data in motion/transit –** Data that is traversing the network and communication cables can be encrypted by using a Transport Layer Security (TLS 1.2 or 1.3) protocol.
- **Data at rest –** Data that is being stored is commonly encrypted using the Advanced Encryption Standard (AES-256) technique.
- **Data in use –** Data that is being used cannot be protected by encryption. To protect data in use, utilize physical controls such as screen protectors, avoid shoulder surfing, face monitors away from windows, lock workstations, and have clean desk and printer policies.

Any potentially sensitive personal data should be encrypted in-motion and at-rest.

Passwords should be encrypted at-rest and files containing encrypted passwords used by systems to authenticate users should be readable only with elevated privileges.

Key management, the management of cryptographic keys, is crucial to the effective use of encryption. Generate, exchange, store, use, replace and delete cryptographic frequently to prevent unauthorized access to those keys.

Incident Management

Incident Management is the process of identifying, managing, recording and analyzing security threats or incidents by utilizing a combination of appliances, systems and human-driven investigation. It is recommended to follow an Incident Management Process with the following basic steps:

1. Planning and preparation – Identify risks and vulnerabilities, proactively remediate issues, and create policies and procedures
2. Detection and analysis – Identify a security event
3. Response or containment – Isolate the threat
4. Mitigation or eradication – Remove the threat from the environment
5. Recovery – Restore system to operational state
6. Reporting – Have an incident response plan and channel for internal and external communication
7. Remediation – Identify the root cause and remediate the issue
8. Lessons learned – Identify what went well and what did not and learn from the mistakes to be better prepared next time

Common Incident Management terminology:

Event – A change in normal behavior of a system such as a system going offline or online, a file dropped to a directory, a security lapse occurs, etc. An event can be positive or negative.

Alert – A monitored event that breached a set condition, generating an alert for further action. A notification of a cybersecurity event.

Incident – An event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization's data.

Problem – An incident that needs to be further analyzed as the cause is unknown.

Digital Forensics is part of the Incident Management Process and relates to the analysis of potentially compromised systems. NIST provides a Computer Forensics Tools and Techniques Catalog that enables practitioners to find tools and techniques based on specific digital forensic functions, such as deleted file recovery and email parsing.

The Federal Financial Institutions Examination Council (FFIEC) provides a full Glossary of defined terms relating to information technology.

The incident response plan should:

- Include a clearly defined process to shut off access to Freddie Mac systems when a Security Incident occurs
- Be tested frequently (at least annually)
- Be reviewed and updated at least annually

Security Orchestration, Automation and Response (SOAR) Tool

SOAR is a set of programs that enables an organization to collect data about security threats and respond to security incidents in a digital workflow format. SOAR allows automated accumulation and flow of security threat data between disparate security technologies (such as SIEM, firewall, incident response platform, etc.). The three stages of SOAR are defined as follows:

Security Orchestration – Connects and integrates internal and external tools using application programming interfaces (APIs) or other means. Connected systems include Firewall, IDS/IPS systems, vulnerability scanners, endpoint protection tools, user behavior analytics, Security Information and Event Management (SIEM) platforms.

- **Security Automation –** Using the data and alerts collected from orchestration, the system ingests and analyzes data and creates repeated, automated processes to replace manual processes.
- **Security Response –** A dashboard provides a single view for responders to help with planning, managing, monitoring, and reporting of actions that are carried out once a threat is detected.

Secure Transmission of Data to Freddie Mac Systems

Ensure the secure transmission of data to Freddie Mac systems. When Application Programming Interface (API)s are used, have policies and procedures in place to authorize and authenticate users and devices. This includes defining access control rules and assigning user access types and using tokens to authenticate API traffic.

Access Management

Access management should include a process for granting and removing system access, requirements for authentication and rules of behavior.

Define remote access requirements including acceptable use, approvals and recertification processes, at least on an annual basis.

Develop and apply an account lock-out threshold that requires that if there are more than five failed login attempts, an account will be locked out until it is reset and/or 24 hours has passed in conjunction with an account lock-out duration setting.

Develop and apply a process to ensure password changes are conducted at least once every 90 days except for system-to-system credentials, which must be conducted at least once every 365 days.

Use multifactor authentication (MFA) for access to every system. Use different factor types from the table below. Do not use two factors from the same type. Use phishing-resistant types of MFA methods such as soft or hard tokens. SMS text or email code MFA methods or not as secure.

Type 1	Type 2	Type 3	Type 4	Type 5
Something you know	**Something you have**	**Something you are**	**Somewhere you are**	**Something you do**
Password, pin, pass phrase	Smart card, token, license	Fingerprint, retina, face scan	IP address, Media Access Control (MAC), location	Signature, pattern, gait

Asset Management

Seller/Servicers must maintain an inventory management system to track physical and software assets such as end-user technology, servers, network devices, and corresponding asset ownership. The inventory management system must be reconciled to actual inventory on a periodic basis to verify all assets are included.

It is also recommended to:

- Determine each asset's status *(e.g.*, active or inactive)
- Identify the life cycle phase of the assets
- Identify personally owned technology assets that are allowed to connect to the network

An inventory management system helps to identify or understand the following:

- License utilization
- Support costs related to maintenance
- Existence of unauthorized devices operating on the network
- Potential vulnerabilities, such as hardware or software that need upgrade or are reaching end-of-life
- Compliance with internal configuration and security standards, as well as contractual requirements
- Critical interdependencies (*e.g.*, third-party service providers, software, hardware and business units)

Automated inventory method tools are available for tracking and validating technology assets. Examples include: ManageEngine AssetExplorer, MMSoft Pulseway, Asset Panda and GoCodes.

Cloud Computing

Cloud computing, in general, is the migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service provides via the Internet "cloud."

The fundamentals of risk and risk management found in the FFIEC Information Technology Examination Handbook apply to cloud computing. However, cloud computing may require more

robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a cloud-computing service provider, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment.

Ensure that the cloud service provider has:

- A strong security infrastructure
- An identity management and authorizations process
- Physical security controls, including a process for natural disasters
- Policies for data back-up and disaster recovery

Vendor Risk Management

An information security and technology risk assessment should be conducted for all third-parties. Best practices include:

- Review cybersecurity policies, standards, controls and procedures and ensure they meet Freddie Mac requirements in Section 2.26 and industry standards
- Review solution architecture and ensure data is protected in transit and at rest
- Request and review independent third-party penetration test report
- Review System and Organization Control (SOC2 Type-2) report to ensure security controls are in place and effectively managed
- Review who has access to data and the level of access
- If there is a fourth-party providing service to the third-party as part of the contract, assess the risk of that engagement

The master service contract should include:

- Service level agreements (SLA) and penalties for SLA deviations
- The right to audit
- Limitations regarding transborder data transfer

Incident Notification to Freddie Mac

In accordance with Section 2.26(c), within 36 hours of incident detection, notify Freddie Mac by completing the Freddie Mac Incident Intake Form. If the Seller/Servicer is unable to access the form, notification may be done via email at Information_Security@FreddieMac.com, Privacy_Incident_Management@FreddieMac.com and MF_Data_Security_and_Privacy@FreddieMac.com.

Notify us even if you are unsure if it is an actual incident/attack. This enables us to assess whether we are seeing something similar in our environment and to stop or minimize any attacks or unauthorized access to information. If it's nothing, no worries! We would much rather confirm there are no issues than have a successful attack occur. Make sure your policies and procedures include this requirement to notify us within 36 hours.

Notify us if you become aware of an incident involving one of your Material Vendors (*i.e.*, those that have access to Freddie Mac data or systems).

Provide us updates and any detail on the incident as soon as possible. We will work closely with our IT teams and ask that you do the same to stay up-to-date. This will also avoid or minimize potential business delays. For example, if we need to cut off access for a secured user account at your organization, quickly providing us evidence that the account is safe will, upon our confirmation and subject to compliance with our own corporate requirements, enable us to lift the access restrictions.

Provide a clear and thorough incident closure report once everything is resolved and all questions from Freddie Mac have been answered. Immediately work on any remediation actions, policy and procedure and training updates.

Other Best Practices

Third-Party Information Security Assessments and Certifications

Completion of third-party and information security assessments and certifications are recommended to show that your organization meets cybersecurity best practices and standards.

SOC report

A cybersecurity System and Organization Control (SOC) report provides organizations with objective assurance that the appropriate systems, processes, and controls exist to manage a cyber incident, enabling stakeholders to make informed decisions. SOC audits are executed by an auditing company and the report is signed/attested by a CPA.

SOC1 – report on controls at a service organization relevant to the internal control over financial reporting (ICFR)

SOC2 – report details the effectiveness of a service organization's controls related to operations and compliance. This report should be labeled and handled as confidential as it may report on security weaknesses

- **Type 1 report –** provides a report of all the procedures and controls within the organization
- **Type 2 report –** a more detailed report that reviews how the organization operated its controls over a period of time and provides an expert opinion on the effectiveness of the controls

SOC3 – a public facing report that provides a high-level overview of the information in the SOC2 report without any information regarding the type of weakness in the identified controls

NIST and ISO Certification

Additional assessments and certifications are also recommended as ways to prove compliance with industry standards. Examples of certifications include those provided by National Institute of Standards and Technology (NIST) and ISO (International Standards Organization).

Cyber Insurance

Cyber insurance may provide coverage for the cost of:

- Conducting incident/breach investigations
- Notifying customers
- Reputational and crisis management
- Business interruption
- Recovering compromised data
- Repairing damaged computer systems
- Credit monitoring for affected customers
- Legal costs