Freddie Mac Information Security Requirements Workbook

Tandem™

Disclaimer: This workbook is for information purposes only. It serves to provide Tandem's opinion of the Freddie Mac information security requirements. Businesses may use this workbook to assist with their compliance preparations, but are encouraged to evaluate the risks and coordinate with appropriate legal counsel before acting on ideas from this document.

Table of Contents

Introduction

How to Use the Freddie Mac Information Security Requirements Workbook

This workbook is designed to help you on your journey towards compliance with Freddie Mac's information security requirements, effective July 3, 2023. Inside this document, you'll find several helpful resources. Here's a sneak peek at how we've got it all mapped out, starting on Page 8.

The section title will go in this colorful bar here at the top.

The official requirements will go over in this navy column.

To simplify things a bit, we're going to put the requirements into some friendly terms and in a checklist format, to boot! Requirements that go into effect in July 2023 will be marked with an icon that looks like this:

To help you learn more, we're also going to include some references to guidance from the FFIEC and NIST. (**Pro Tip:** Click the section name to open the guidance!)

This section will show products, features, and other resources from Tandem where you can learn more about the topics, as well.

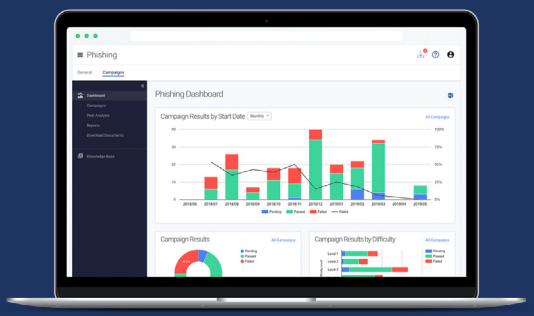
If there's room, we may also include some peer data, trivia, information security fun facts, or Tandem product spotlights related to the topic at hand.

We know information security compliance can be a lot, so instead of trying to read this entire workbook cover-to-cover, we encourage you to use the sections on an as-needed basis. For example, if you plan to work on your vulnerability management practices, you could refer to Page 17 for some guidance, at that time.

We hope you find this workbook helpful. If you have questions or would like more information about how Tandem can help you comply with information security requirements, email us at info@tandem.app or visit our website, Tandem.App/Contact.

About Tandem

Tandem is an information security and compliance software-as-a-service created to help financial institutions improve information security, stay in compliance, and lower overhead costs. Find out how Tandem can help you at Tandem.App.



DID YOU KNOW?

Freddie Mac has roots dating all the way back to 1938.

- **1938**
  The Federal National Mortgage Association ("Fannie Mae") was founded during the Great Depression, as part of the New Deal. The goal was to increase home ownership and stimulate the economy.
- **1968**
  Fannie Mae was split in two: One side kept the Fannie Mae name, while the other side came to be known as the Government National Mortgage Association ("Ginnie Mae").
- **1970**
  To make sure Fannie Mae didn't have a monopoly, Congress started Freddie Mac to promote competition and make more funds available for lenders.
- **1989**
  Freddie Mac got the official go-ahead from Congress to sell stock and became a publicly traded company.
- **2008**
  When the mortgage crisis happened, the U.S. Government stepped back in and put Freddie Mac under conservatorship.
- **2023**
  As of today, Freddie Mac operates as a publicly traded, government-sponsored enterprise (GSE).

About the Requirements

The Federal Home Loan Mortgage Corporation ("Freddie Mac") information security requirements can be found in Section 1302.2 of The Single-Family Seller Servicer Guide (a.k.a., "the guide").

Any organization that acts as a seller or servicer of loans sold to Freddie Mac is expected to comply with the requirements established in the guide. (They're pretty serious about it, too. Failure to comply with the requirements may result in the termination of a financial institution's right to sell or service mortgages.)

A Brief History

2016

May 2, 2016 was the effective date for the first "minimum standards" for an information security program. The guide recommended maintaining information security policies and procedures, as well as implementing physical, technical, and administrative controls.

2020

October 1, 2020 was the effective date for a modification. Each business needed to not only maintain their own information security program, but they needed to expect their third parties to implement procedures to promote information security, as well.

2022

January 13, 2022 was the effective date for another modification. This update included a requirement to notify Freddie Mac within 48 hours of experiencing a security incident. This update also featured some additional changes to the third party requirements.

2023

July 3, 2023 is the effective date for the latest version of the requirements. These requirements include several new security concepts and best practices for ensuring the confidentiality, integrity, and availability of systems and information.

Related Agencies

Of course, you know Freddie Mac. (If you don't, go back a page.) But did you know that the guide refers to two external agencies in Section 1302?

These agencies are some of the leading providers of detailed guidance on the components of a successful information security program. This workbook provides resources from these other agencies to help make sure your bases are covered.

FFIEC

Federal Financial Institutions Examination Council

The FFIEC is an interagency council with representation from each of the federal banking agencies. The following agencies are represented on the FFIEC.

- Board of Governors of the Federal Reserve System (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- National Credit Union Association (NCUA)
- Office of the Comptroller of the Currency (OCC)
- Consumer Financial Protection Bureau (CFPB)
- State Liaison Committee (SLC)
    - Conference of State Bank Supervisors (CSBS)
    - American Council of State Savings Supervisors (ACSSS)
    - National Association of State Credit Union Supervisors (NASCUS)

According to their website, "the FFIEC prescribes uniform principles, standards, and report forms for the federal examination of financial institutions." This includes the FFIEC Information Technology (IT) Examination Handbook and the Cybersecurity Assessment Tool (CAT).

NIST

National Institute of Standards and Technology

The mission of NIST is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

Part of NIST is the Information Technology Laboratory (ITL). This division specializes in developing standards and resources to help organizations improve their security. Some of their most well-known resources include the Special Publication (SP) 800 series, which features a variety of guidance and control frameworks, and the NIST Cybersecurity Framework (CSF).

TRIVIA

How many booklets are part of the FFIEC IT Examination Handbook?

(Check your answer on Page 28.)

DID YOU KNOW?

The FFIEC Cybersecurity Assessment Tool (CAT) has seen a steady increase in adoption by financial institutions over the last four years.

Institutions who use the FFIEC CAT:

- 2022 (91%)
- 2021 (89%)
- 2020 (82%)
- 2019 (81%)

Source: Tandem State of Cybersecurity Report (2022)

Definitions

The guide features several key "legal" terms that will be used in this document. For clarity, let's go ahead and define those here, so you can come back and reference them, if needed.

Freddie Mac Confidential Information

"Freddie Mac confidential information may include, but is not limited to, information and documentation concerning the development, negotiation, operation or terms of various products or programs, technology, business terms, trade secrets and commercial and financial information. In addition, information that Seller/Servicer is required by applicable law to treat as confidential, and information that Seller/Servicer knows or should know should be treated as confidential are considered Freddie Mac confidential information, whether or not Freddie Mac has identified the information as confidential. (See the full definition in the guide Section 1201.8(a).)"

Protected Information

"Through its Servicing of Mortgages for Freddie Mac, the Servicer may obtain information, including fair lending data elements, concerning the Borrower or the Mortgaged Premises (i.e., the land and improvements thereon subject to the lien of a Security Instrument) that either is not publicly available or that is required to be protected under applicable privacy, securities, information security, consumer protection or other laws. (See the full definition in the guide Section 8101.8.)"

Related Third Party

"A third party (i.e., a Seller/Servicer counterparty such as a Mortgage Broker, Correspondent, loan origination system vendor, contract underwriter, appraisal management company, data center, settlement agent, third-party provider (TPP), Selling Agent, Servicing Agent, Document Custodian, Warehouse Lender, Outsourced Vendor, mortgage insurer or reinsurer) that the Seller/Servicer engages to provide it with technology, origination, underwriting, processing, technical, interim financing, closing, loss mitigation, (re)insurance, servicing and other services and support that are generally designed to advance the Seller/Servicer's origination and/or Servicing of Mortgages."

Security / Privacy Incident

"If a Seller/Servicer knows or believes, or if a reasonable information or cyber security professional could conclude from the circumstances and available information, that (a) there has been any unauthorized acquisition of data or computing resources, or unauthorized access to data or computing resources or any other security related issue that may compromise the security, confidentiality, availability, integrity or privacy of Freddie Mac confidential information or Protected Information ("Security Incident") or (b) Freddie Mac confidential information or Protected Information has been exposed, accessed or used without authorization ("Privacy Incident"), the Seller/Servicer must follow the requirements" in the Privacy Incident Notification and Security Incident Notification sections below.

System

"Individually and collectively, a Freddie Mac-owned, -leased, -licensed or -controlled technology platform whether or not identified in a System-Specific License including, without limitation, Distributed Code, Specifications, any related computer, other hardware or electronic device, application or operating system software, web site, private data or other communication network, interface (including any application programming interface, or "API" created and hosted by Freddie Mac to facilitate back-end access to its systems) and/or connectivity which, in each instance, Freddie Mac provides or makes available to the Seller/Servicer in connection with the Purpose. (See the full definition in the guide Section 2401.1.)"

Information Security Program

Checklist

- [ ] Designate a person (or a committee) to oversee the information security program at your company.
- [ ] At a minimum, ensure the program addresses:
  - Acceptable Use
  - Ownership of and access to information
  - Baseline security practices
  - Physical, administrative, and technical controls
- [ ] Review the information security program at least annually.
- [ ] Keep the information security program at the ready. Be prepared to attest that it is "adequate," if Freddie Mac asks you about it.

Resources

FFIEC Information Security Booklet

- Section I.B Responsibility and Accountability
- Section II.C.3 Control Types
- Section II.C.7 User Security Controls

FFIEC Management Booklet

- Section I.B.2 Information Security

Tandem Mapping

Tandem Policies

- Acceptable Use Policy
- Security Committee

Tandem Information Security Program Resource

Tandem Blog

- 6 Key Qualities of ISOs According to the FFIEC
- Understanding the Role of an ISO
- 4 Things to Consider Before Hiring a Virtual ISO (vISO)
- ISO Management and Staffing in 2021
- What to Do if Your ISO Leaves

FREDDIE MAC GUIDE 1302.2(b)(i)

Seller/Servicers must define an individual or group of individuals responsible for the development of information security requirements, including the adoption, implementation, maintenance and administration of written minimum-security standards, policies and procedures that responsibly address critical issues such as user responsibilities (e.g., "Acceptable Use"); ownership of and access to information; baseline security practices; physical, administrative and technical security protection mechanisms and other requirements.

Not less than annually, Seller/Servicers must review and assess the adequacy of their information security policies and procedures used in connection with the selling and Servicing of Freddie Mac Mortgages to ensure compliance with the Guide, their other Purchase Documents and industry best practices (including as set forth by the Federal Financial Institutions Examination Council and National Institute of Standards in Technology). Upon request of Freddie Mac, Seller/Servicers must make their information security program policies and procedures available and provide an attestation of the adequacy of these policies and procedures, including following Freddie Mac's termination of a Seller/Servicer's right to sell or service Mortgages.

DID YOU KNOW?

Financial institutions fill the Information Security Officer (ISO) role in a variety of ways.

- ISO is one person (69%)
- ISO is a department (13%)
- ISO is a committee (13%)
- ISO is outsourced (4%)

Source: Tandem State of Cybersecurity Report (2022)

Human Resources Security

FREDDIE MAC GUIDE 1302.2(b)(ii)

Pre-employment screening: Seller/Servicers must conduct, or retain a qualified third party to conduct, thorough background verification checks (screening) for all candidates for employment or contractor status who will have access to Freddie Mac confidential information, Protected Information or Systems.

Code of conduct or non-disclosure agreement: Prior to being granted access to Freddie Mac confidential information, Protected Information or Systems, Seller/Servicers must require all employees, contractors and third parties to (i) sign a non-disclosure agreement or (ii) be subject to a code of conduct, which in either case includes obligations to restrict the use or disclosure of and to maintain as confidential all Freddie Mac confidential information.

Protected Information and information related to or contained in Systems: The code of conduct must be acknowledged by the employee, contractor or third party, and must address at least the following subjects:

- Appropriate use of company assets
- Information protection, including non-disclosure and confidentiality
- Records management
- Information security and privacy
- Business courtesies
- Personal investments and insider trading
- Conflicts of interest

Information security awareness, education and training: At least annually, Seller/Servicers must provide information security awareness training to all employees, contractors and third parties who have access to Freddie Mac confidential information, Protected Information and/or Systems. The awareness training must be current in substance and reflect up-to-date vulnerabilities, threats and techniques, including information about phishing campaigns and techniques. At a minimum, the training must provide details on roles and responsibilities for all users in protecting information at the Seller/Servicer, along with practical ways to incorporate information security into daily routines.

Checklist

For employees, contractors, and third parties who will have access to confidential information or systems:

- ☐ Do (or hire someone to do) background checks on prospective hires. *(This one does not apply to third parties.)*
- ☐ Require them to sign a nondisclosure agreement (NDA) or code of conduct.
- ☐ Ensure the code of conduct covers appropriate topics around acceptable use, information security, and ethics.
- ☐ Provide training at least annually. Make sure the training includes:
  - Current events and considerations (like phishing).
  - Roles and responsibilities for security.
  - Practical ways to incorporate security into daily work.

Resources

FFIEC Information Security Booklet

- Section II.C.7 User Security Controls
- Section II.C.7(a) Security Screening in Hiring Practices
- Section II.C.7(e) Training

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section VI.A.4 Personnel Controls

NIST Cybersecurity Framework: PR.AT Category (PR.AT-1 - PR.AT-5)

Tandem Mapping

Tandem Policies

- Employee Security Awareness Training
- Personnel Security
- Vendor Management

Tandem Risk Assessment Controls

- Background Checks
- Employee Security Awareness Training

Tandem Blog: 5 Ways to Improve Your Phishing Test Results

Physical & Environmental

Checklist

- [ ] Have a plan to prevent, detect, and respond to physical security incidents.
- [ ] Make sure your facilities have appropriate alarm systems and surveillance equipment.
- [ ] Keep a list of people approved to access the facilities where your physical systems live. ❗
- [ ] Review the list at least annually and when someone on the list departs the business. ❗
- [ ] Implement environmental controls to make sure you don't lose connections, information, or facilities if a natural disaster strikes.

Resources

FFIEC Business Continuity Management Booklet

FFIEC Information Security Booklet

- Section II.C.7(b) User Access Program
- Section II.C.8 Physical Security
- Section II.C.13(a) Storage

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section V.B Network and Telecommunications
- Section V.D Environmental Controls
- Section V.E Physical Access Controls

NIST Cybersecurity Framework: PR.AC-2, PR.IP-5, DE.CM-2

Tandem Mapping

Tandem Policies

- Access Control
- Personnel Security

Tandem Business Continuity Plan Preparedness Controls

- Alarm Systems
- Alternate Data Center
- Heating, Ventilation, and Air Conditioning (HVAC)

FREDDIE MAC GUIDE 1302.2(b)(iii)

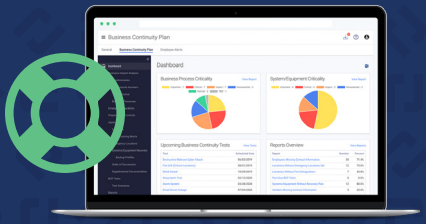
Seller/Servicers must create and maintain:

- A physical security control program of the organization's buildings and facilities that contain information systems, designed to detect, monitor and prevent unauthorized access and to respond to physical security incidents using real-time physical intrusion alarms and surveillance equipment.
- An updated list of personnel with authorized access to facilities where information systems reside, including an access privilege review performed not less than annually and upon the departure of any authorized personnel.
- Environmental controls to monitor, mitigate against and protect the organization with regards to a loss of connectivity, access to or integrity of information and damage caused by natural disasters or man-made incidents such as fire, earthquake, flood, hurricane, tornado or weather-related adverse conditions.

PRODUCT SPOTLIGHT

Tandem Business Continuity Plan is designed to help you manage and protect operations before, during, and after a business disruption.

See how Tandem can help disaster-proof your business at Tandem.App/Business-Continuity-Planning.



Communications & Ops. Mgmt.

FREDDIE MAC GUIDE 1302.2(b)(iv)

Seller/Servicers must implement technical security measures designed to monitor for, mitigate against and prevent malicious software, stop unwanted spam and traffic and to protect against unauthorized use of wireless connections. Measures must include those provided in the remainder of this section or meet industry best practices, whichever is more stringent.

FUN FACT

While the phrase "monitor for, mitigate against, and prevent" might be new in the requirements, this is not a new concept in the world of security.

These three ideas can be directly mapped to NIST's "Five Functions" in the Cybersecurity Framework (CSF).

The Five Functions are:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

To most effectively promote security, and reduce the risk of threats like malware, businesses are encouraged to implement controls in each of these areas.

Checklist

- [ ] Implement measures to monitor for, mitigate against, and prevent malware.
- [ ] Implement an anti-malware solution.
- [ ] Implement spam / email filtering.
- [ ] Implement border protection (e.g., firewalls, content filters, etc.).
- [ ] Prohibit unauthorized wireless connections.

Resources

FFIEC Information Security Booklet

- Section II.C.9 Network Controls
- Section II.C.9(a) Wireless Network Considerations
- Section II.C.12 Malware Mitigation

FFIEC Architecture, Infrastructure, and Operations Booklet

- VI Operations

NIST Cybersecurity Framework: DE.CM-4, DE.CM-7

Tandem Mapping

Tandem Policies

- Email Security
- Firewall
- Intrusion Detection and Prevention
- Malicious Software Protection
- Wireless Network Access

Tandem Risk Assessment Controls

- Anti-Malware Software
- SPAM Filter

Data Transmission & DLP

Checklist

- [ ] Implement controls for data loss prevention (DLP). (This often includes controls like data classification, security awareness training, encryption, email and web filtering solutions, disabling or restricting USB ports, etc.)
- [ ] Have policies that address securing information exchange. (This often includes policies for things like encryption, email security, data storage, removable media, etc.)
- [ ] Make sure any software you use for DLP is up to date.
- [ ] Scan for sensitive information stored on disks.
- [ ] Scan for sensitive information transmitted over public communication paths.
- [ ] Restrict transfer of data to removable media.

Resources

FFIEC Information Security Booklet

- Section II.C.9 Network Controls
- Section II.C.13(a) Storage
- Section II.C.19 Encryption

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section V.B.1 Network

NIST Cybersecurity Framework: PR.DS-5

Tandem Mapping

Tandem Policies

- Employee Security Awareness Training
- Encryption
- Email Security
- Removable Media and Data Transfer

Tandem Risk Assessment Controls: Data Loss Prevention (DLP) Program

FREDDIE MAC GUIDE 1302.2(b)(v)

Seller/Servicers must:

- Maintain a data loss prevention/ transmission protection mechanism and related written policy establishing requirements to protect the confidentiality and integrity of information exchange using technology applications or information systems.
- Ensure adequate and up-to-date data loss prevention software is used and a corresponding management process is in place to scan for sensitive information stored on media and outgoing transmissions over public communication paths as well as to restrict the transfer of data to USB and other removable media devices at the desktop level.

SOME HELPFUL DEFINITIONS

Data Loss Prevention (DLP) Program

"A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data while it is stored, used, or in transit over the network and at the perimeter." (FFIEC)

Removable Media

"Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD)." (NIST)

Anti-Virus Program / Updates

FREDDIE MAC GUIDE 1302.2(b)(vi)

Seller/Servicers must install anti-virus software to protect servers and end user systems and must keep all such software up to date with the latest anti-virus software and definitions.

Checklist

- [ ] Install anti-virus on servers and employee devices (e.g., workstations, laptops, mobile devices, etc.).
- [ ] Keep anti-virus software up-to-date.

Resources

FFIEC Information Security Booklet

- Section II.C.12 Malware Mitigation
- Section II.C.15(d) Use of Remote Devices

FFIEC Joint Statement on Destructive Malware

NIST Cybersecurity Framework: DE.CM-4

Tandem Mapping

Tandem Policies: Malicious Software Protection

Tandem Risk Assessment Controls: Anti-Malware Software

FUN FACT

While the terms "anti-virus" and "anti-malware" have historically been used as synonyms, anti-virus is now often considered to be a more specialized form of anti-malware. Anti-virus is often associated with signature based virus detection, whereas anti-malware offers greater ability to prevent, detect, and respond to emerging types of malicious software.

DEFINITION

Anti-Malware Software

"Anti-malware applications are part of the common secure configurations for system components. Anti-malware software employs a wide range of signatures and detection schemes, automatically updates signatures, disallows modification by users, run scans on a frequently scheduled basis, has an auto-protect feature set to scan automatically when a user action is performed (e.g., opening or copying a file), and may provide protection from zero-day attacks. For platforms for which anti-malware software is not available, other forms of anti-malware such as rootkit detectors may be employed." (NIST)

Network Security

Checklist

- [ ] Implement firewalls to protect data entering and leaving the network.
- [ ] Disable unused ports, protocols, and services.
- [ ] Review and reauthorize firewall rules at least annually and when significant changes happen to your network.

Resources

FFIEC Information Security Booklet

- Section II.C.9 Network Controls
- Section II.C.15(c) Remote Access
- III Security Operations

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section V.B.1 Network
- Section V.B.2 Telecommunications

NIST Cybersecurity Framework: PR.AC-5, PR.PT-4, DE.CM-1

Tandem Mapping

Tandem Policies

- Firewall
- Intrusion Detection and Prevention
- Network Monitoring and Log Management

Tandem Risk Assessment Controls

- Firewall
- Internal Network Monitoring
- Intrusion Detection/Prevention System

FREDDIE MAC GUIDE 1302.2(b)(vii)

Seller/Servicers must:

- Implement information technology controls such as stateful firewalls to block all traffic inbound from, and outbound to, public networks that have not been expressly permitted by policy (i.e., "deny by default").
- Manage and restrict ports, protocols, and services to only those that are required and approved for business operations.
- Formally recertify and authorize firewall rules upon each significant change (including, but not limited to, physical appliance updates, firmware updates and other changes to firewall technology) in infrastructure and otherwise not less than annually.

DID YOU KNOW?

91.2% of financial institutions say they audit or verify their firewall rules at least quarterly.

Source: Tandem Cybersecurity Assessment Tool Peer Analysis (04/2023)

Mobile Computing

FREDDIE MAC GUIDE 1302.2(b)(viii)

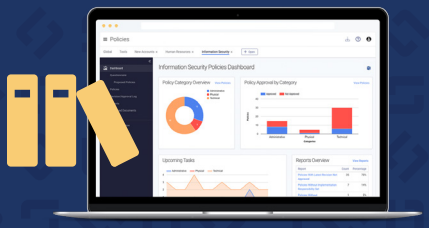
Seller/Servicers must maintain a written mobile device/computing management (MDM) policy that has been approved by management and communicated to all appropriate personnel. This policy must reflect current and best practices, specifying parameters including but not limited to:

- Approved and prohibited applications
- Cryptographic mechanisms to ensure data security
- Identity and access management requirements
- Software updates

PRODUCT SPOTLIGHT

Tandem Policies is designed to help you create and maintain your information security policies. With Tandem's template list of 50+ information security policies, you can maintain a living set of policies that is easily accessible.

See how Tandem can help improve your policies at Tandem.App/Policies-Management-Software.



Checklist

- [ ] Have a written Mobile Device Management (MDM) policy.
- [ ] Get it approved by management.
- [ ] Communicate it to all appropriate personnel.
- [ ] Make sure it addresses things like:
  - Approved and prohibited applications
  - Encryption
  - Access control
  - Patch management

Resources

FFIEC Information Security Booklet

- Section II.C.10(b) Hardening
- Section II.C.10(d) Patch Management
- Section II.C.17 Application Security

NIST Cybersecurity Framework: PR.AC-1, DE.CM-7

Tandem Mapping

Tandem Policies: Mobile Device Management (MDM)

Wireless Networks

Checklist

- [ ] Control, secure, and monitor wireless access points.
- [ ] Require strong authentication for access to wireless networks.
- [ ] Ensure wireless traffic is encrypted with strong encryption.
- [ ] Prohibit outdated wireless encryption technology.
- [ ] Review approved wireless networks at least annually to verify only authorized users and access points are connected.
- [ ] Require authentication to access routers.
- [ ] Limit, monitor, and control administrator access to routers.

Resources

FFIEC Information Security Booklet

- Section II.C.9 Network Controls
- Section II.C.9(a) Wireless Network Considerations

NIST Cybersecurity Framework: PR.AC-5, PR.PT-4

Tandem Mapping

Tandem Policies: Wireless Network Access

FREDDIE MAC GUIDE 1302.2(b)(ix)

Seller/Servicers must control, secure, and monitor wireless access points. In addition, Seller/Servicers that offer wireless networks for network users must:

- Implement and keep up to date a strong Wireless Local Area Network (WLAN) Authentication method that meets or exceeds the current industry standard Encryption strength and technology.
- Prohibit use of outdated wireless technologies such as Wired Equivalent Privacy (WEP).
- At least annually, perform reviews of approved wireless networks to validate and verify authorized users and access points.
- Password protect and control administrative access to the router.

Vulnerability Management

FREDDIE MAC GUIDE 1302.2(b)(x)

Seller/Servicers must conduct vulnerability testing on a regular basis and have a process in place to analyze and remediate identified vulnerabilities. To accomplish this, the Seller/Servicer must:

- Not less than annually, employ a qualified and independent third party to conduct penetration testing on systems or system components used to store, access, process and/or transmit Freddie Mac confidential information or Protected Information or connect to Systems.
- Maintain a written vulnerability assessment process and policy that has been approved by management, communicated to appropriate personnel and has an owner that implements, maintains and reviews the policy at least annually to ensure that it consistently reflects industry best practices.
- Remediate all identified vulnerabilities.
- Maintain a record of all identified vulnerabilities and their remediation status.

DID YOU KNOW?

96.5% of financial institutions say they conduct independent testing (including penetration testing and vulnerability scanning) according to their organization's risk assessment.

Source: Tandem Cybersecurity Assessment Tool Peer Analysis (04/2023)

Checklist

- [ ] Hire an independent third party to perform penetration testing at least annually.
- [ ] Have a vulnerability assessment policy and process.
- [ ] Get it approved by management.
- [ ] Review and update the policy at least annually.
- [ ] Conduct vulnerability assessments on a regular basis.
- [ ] Fix identified vulnerabilities.
- [ ] Keep a record of identified vulnerabilities and their status.

Resources

FFIEC Information Security Booklet

- Section II.A.2 Vulnerabilities
- Section II.C.10(d) Patch Management
- Section IV.A.2(b) Penetration Tests
- Section IV.A.2(c) Vulnerability Assessments

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section VI.B.3 Vulnerability and Patch Management

NIST Cybersecurity Framework: ID.RA-1, PR.IP-12 DE.CM-8, RS.AN-5, RS.MI-3

Tandem Mapping

Tandem Policies: Vulnerability and Patch Management

Tandem Risk Assessment Controls: Vulnerability Scans

Configuration & Patch Mgmt.

Checklist

- [ ] Have a written patch management policy and process.
- [ ] Get it approved by management.
- [ ] Communicate it with all appropriate personnel.
- [ ] Review and update the policy on a regular basis.
- [ ] Have a process for creating secure configuration baselines.
- [ ] Implement intrusion detection / prevention systems (IDS / IPS).
- [ ] Implement email filtering with attachment blocking.
- [ ] Designate responsibility for performing patch management.
- [ ] Test and install software patches and updates on a timely basis.

Resources

FFIEC Information Security Booklet

- Section II.C.10 Change Management within the IT Environment
- Section II.C.10(a) Configuration Management
- Section II.C.10(b) Hardening
- Section II.C.10(c) Standard Builds
- Section II.C.10(d) Patch Management

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section VI.B.2 Configuration Management
- Section VI.B.3(b) Patch Management

NIST Cybersecurity Framework: PR.PT-3, PR.IP-1, PR.IP-3

Tandem Mapping

Tandem Policies

- Change Management
- Intrusion Detection and Prevention
- Vulnerability and Patch Management

Tandem Risk Assessment Controls: Change Management

FREDDIE MAC GUIDE 1302.2(b)(xi)

Seller/Servicers must:

- Implement and maintain a written patch management process and a policy that has been approved by management, communicated to all appropriate personnel and has a designated owner that reviews, implements and maintains the policy to ensure that it consistently reflects industry best practices.
- Develop and execute a process for developing and maintaining secure configuration baselines (also known as hardening guides, baseline secure configurations) of infrastructure components.
- Deploy intrusion detection and/or prevention systems (IDS and IPS) patch management with generated events fed into centralized systems for analysis.
- Define, implement and maintain preventive controls designed to block malicious messages and attachments from entering the environment.
- Designate qualified personnel responsible for performing timely software updates and patches and maintain a process for testing and installing software updates as they become available.

Auditing, Logging, & Monitoring

FREDDIE MAC GUIDE 1302.2(b)(xii)

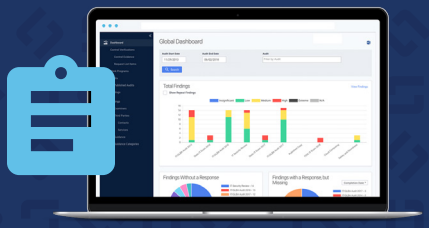
Seller/Servicers must:

- Develop, implement and maintain written guidelines and requirements for the logging and monitoring of activities and action within information systems. If the Seller/Servicer uses an enterprise log management function, the subject requirements must be integrated with such log management function.
- Develop, implement and maintain written log retention and handling requirements to ensure logs retain relevant, useable and timely information sufficient to identify user access and/or system activities.
- Perform an independent security assessment of the control environment not less than annually and upon the occurrence of any data Security Incident or Privacy Incident (defined below).

PRODUCT SPOTLIGHT

Tandem Audit Management streamlines the process of responding to audits, helping standardize your documentation and ensuring identified issues are addressed.

See how Tandem can help improve your finding response process at Tandem.App/Audit-Management-Software.



Checklist

- ☐ Have written guidelines for logging and monitoring.
- ☐ Create written log retention and handling requirements.
- ☐ Have an independent controls audit at least annually and in the event of a security or privacy incident.

Resources

FFIEC Information Security Booklet

- Section II.C.22 Log Management
- Section II.D Risk Monitoring and Reporting
- Section IV.A.2(d) Audits

Specific examples of monitoring are addressed throughout the booklet.

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section II.D Internal Audit, Independent Reviews, & Certification Processes
- Section VI.B.7 Log Management
- Section VI.D Ongoing Monitoring and Evaluation Processes

NIST Cybersecurity Framework: PR.PT-1

Tandem Mapping

Tandem Policies

- Network Monitoring and Log Management
- Security Testing

Tandem Audit Management

Software Development (SDLC)

Checklist

If the organization develops applications or software:

- [ ] Have a written SDLC policy and process.
- [ ] Get it approved by management.
- [ ] Make sure the policy addresses things like:
    - Separate production and testing environments
    - Secure coding
    - Open-source
    - Code deployment best practices

Resources

FFIEC Information Security Booklet

- Section II.C.17 Application Security

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section V.C.1 Internally and Externally Developed Software

FFIEC Development & Acquisition Booklet

- System Development Life Cycle Section

NIST Cybersecurity Framework: PR.DS-7, PR.IP-2

Tandem Mapping

Tandem Policies: Third-Party Secure Application Development

Tandem Risk Assessment Controls:

- Code Review
- Secure Coding Techniques

FREDDIE MAC GUIDE 1302.2(b)(xiii)

If a Seller/Servicer develops applications or software that store, access, process or transmit Freddie Mac confidential information, Protected Information or connects to Systems, the Seller/Servicer must develop, implement and maintain a written SDLC process and policy that has been approved by management. This policy must include at minimum:

- Management and separation of production and development environments that reflect contemporary best practices
- Secure coding requirements
- Open-source requirements
- Code development and scanning pre- and post-deployment

FUN FACT

The **Open Worldwide Application Security Project (OWASP)** is a non-profit foundation that works to improve the security of software.

Check out their OWASP Secure Coding Practices - Quick Reference Guide to learn about general software security coding best practices.

Data Encryption

FREDDIE MAC GUIDE 1302.2(b)(xiv)

Seller/Servicers must:

- Maintain a formal Encryption and cryptography use policy that has been approved by management, has been communicated to appropriate personnel and has an owner that implements, maintains and reviews the policy to ensure it consistently reflects industry best practices.
- Ensure the protection, integrity and confidentiality of Freddie Mac confidential information and Protected Information in transit and at rest.
- Deploy cryptography standards that meet or exceed the then-current industry standard Encryption strength and technology and prohibit use of outdated technologies.
- Use Encryption mechanisms on portable end-user devices to protect data if the hardware (laptop, mobile device, etc.) is lost or stolen.
- Deploy data-at-rest and data-in-transit Encryption or commensurate data protections for Freddie Mac confidential information and Protected Information.

DID YOU KNOW?

99% of financial institutions say confidential data are encrypted when transmitted across public or untrusted networks (e.g., internet).

Source: Tandem Cybersecurity Assessment Tool Peer Analysis (04/2023)

Checklist

- ☐ Have a written encryption policy.
- ☐ Get it approved by management.
- ☐ Train personnel on the policy requirements.
- ☐ Review the policy on a regular basis.
- ☐ Encrypt confidential information at-rest and in-transit.
- ☐ Ensure encryption standards used meet or exceed current standards.
- ☐ Do not use outdated encryption technology.

Encrypt portable end-user devices (e.g., phones, laptops, etc.).

Resources

FFIEC Information Security Booklet

- Section II.C.19 Encryption

Tandem Mapping

Tandem Policies: Encryption

Tandem Risk Assessment Controls: Data Encryption

Incident Management

Checklist

- ☐ Develop an incident response plan.
- ☐ Make sure that the plan:
  - Includes playbooks for incident response.
  - Defines needed resources.
  - Defines roles and responsibilities.
- ☐ Test the plan annually.

Resources

FFIEC Information Security Booklet

- Section III.C Incident Identification and Assessment
- Section III.D Incident Response

FFIEC Architecture, Infrastructure, and Operations Booklet

- VI.C.4 Event, Incident, and Problem Management

FFIEC Business Continuity Management Booklet

- V.F.1 Incident Response
- VII Exercises and Tests

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide

NIST Cybersecurity Framework: PR.IP-9, RS.RP-1

Tandem Mapping

Tandem Incident Management

Tandem Policies: Incident Management

Tandem Risk Assessment Controls: Incident Response Plan

Tandem Blog

- 6 Phases of an Effective Incident Response Plan
- Incident Response Plan Communication Guidelines
- Ransomware Incident Response Playbook
- Security Incident Management Training: What Employees Need to Know
- Third-Party Incident Response Playbook

FREDDIE MAC GUIDE 1302.2(b)(xv)

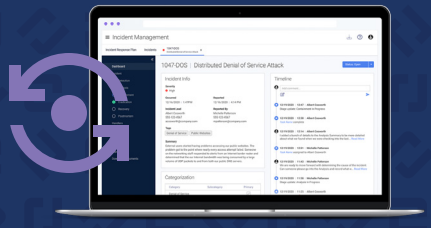
Seller/Servicers must:

- Develop and maintain, and implement when triggered, an incident response plan that provides a roadmap for implementing incident response capabilities and defines the resources and management support needed.
- Annually, unless formally activated, test the effectiveness of the incident response plan and capabilities.

PRODUCT SPOTLIGHT

Tandem Incident Management streamlines the process of creating an incident response plan and helps you track incidents, when they occur.

See how Tandem can improve your incident management practices at Tandem.App/Incident-Management-Software.



Secure Data Transmission

FREDDIE MAC GUIDE 1302.2(b)(xvi)

Seller/Servicers must not transmit to Systems, through an API or otherwise, any materials that contain bugs, viruses, worms or other functions, routines, devices or instructions that may create any unauthorized access, or damage the protection, integrity and confidentiality of data in transit.

Checklist

- [ ] Do not intentionally transmit malicious content to systems.
- [ ] Perform due diligence on APIs before use.

Resources

FFIEC Information Security Booklet

- Section II.C.13(b) Electronic Transmission of Information
- Section II.C.15 Logical Security

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section V.B Network and Telecommunications
- Section V.C.2(c) Application Programming Interfaces
- Section VI.C.2 Operational Support

NIST Cybersecurity Framework: PR.DS-2

Tandem Mapping

Tandem Policies

- Acceptable Use Policy
- Removable Media and Data Transfer
- Vendor Management

DID YOU KNOW?

54% of financial institutions say they are "**Extremely**" or "**Very**" confident in their ability to detect an incident as it is happening.

- Extremely Confident (9%)
- Very Confident (45%)
- Somewhat Confident (37%)
- Slightly Confident (8%)
- Not at All Confident (1%)

Source: Tandem State of Cybersecurity Report (2022)

Access Control

ACCESS MANAGEMENT POLICY

Checklist

- ☐ Have an access management policy and process.
- ☐ Require strong authentication for users with elevated privileges, including administrators.
- ☐ Require strong authentication for remote users.
- ☐ Train remote users on acceptable use of remote resources.
- ☐ Review and re-approve remote authorizations on a regular basis.
- ☐ Require strong authentication after multiple failed login attempts.
- ☐ Implement session timeout controls.
- ☐ Grant access based on the principle of least privilege.
- ☐ Require multi-factor authentication, when applicable.
- ☐ Monitor account access for users who transfer roles, are terminated, or no longer need access to their accounts.
- ☐ Notify Freddie Mac within one business day of transfer or termination of a user who had access to confidential information or systems.
- ☐ Comply with access control instructions on this website: https://sf.freddiemac.com/tools-learning/technology-login

Resources

FFIEC Authentication and Access to Financial Institution Services and Systems Guidance

FFIEC Information Security Booklet

- Section II.C.7 User Security Controls
- Section II.C.7(b) User Access Program
- Section II.C.9 Network Controls
- Section II.C.9(a) Wireless Network Considerations
- Section II.C.10(b) Hardening
- Section II.C.15(a) Operating System Access
- Section II.C.15(b) Application Access
- Section II.C.15(c) Remote Access

See additional access control resources on the next page.

FREDDIE MAC GUIDE 1302.2(b)(xvii)(A)

Access management policy

A Seller/Servicer must:

- Establish, implement and maintain an access management policy that aligns with industry best practices, including a process for granting and removing system access, requirements for Authentication and rules of behavior.
- Define and enforce access and authentication requirements for system administrators and other privileged accounts.
- Define and enforce remote access requirements, including acceptable use, approvals and recertification processes.
- Define and enforce requirements around locked accounts after multiple failed login attempts and timeout requirements.
- Establish and enforce access control methods that limit access to systems, physical or virtual resources and grant access to users on a need-to-know basis.
- Define and enforce requirements for multi-factor authentication where applicable (privileged sessions, remote connectivity, applications housing Freddie Mac confidential information or Protected Information, etc.).
- Manage user accounts for Systems, in accordance with the Guide and the other Purchase Documents. Seller/Servicers must monitor account access for users who transfer roles or are terminated or no longer need access to their accounts. Seller/Servicers must notify Freddie Mac (see Directory 8) within one Business Day after any transfer or termination.

Refer to and comply with the instructions to update systems access for relevant applications at https://sf.freddiemac.com/tools-learning/technology-login.

Access Control

GRANTING, REMOVING, & REVIEWING ACCESS

FREDDIE MAC GUIDE 1302.2(b)(xvii)(B)

Granting, removing and reviewing access

Seller/Servicers must maintain and enforce written procedures for the following:

- Approval of access requests.
- Removal of access for terminations and transfers.
- Analysis of user access and removal of access that is inactive or no longer needed.
- At least annual review of all user access privileges and certification of access according to the minimum information necessary to access permission rules.
- Prohibit or prevent using the same service account identifiers and passwords in both production and non-production environments.

Checklist

Make sure your procedures address things like:

- [ ] Approving access requests.
- [ ] Removing access when it is no longer needed.
- [ ] Reviewing and re-approving user access at least annually.
- [ ] Prohibiting service accounts from running with the same usernames and passwords in test and production environments.

Additional Resources

FFIEC Architecture, Infrastructure, and Operations Booklet

- III.G Remote Access
- V.E Physical Access Controls
- VI.A.3 Identity and Access Management

FFIEC Joint Statement on Cyber Attacks Compromising Credentials

NIST Cybersecurity Framework: PR.AC Category (PR.AC-1 - PR.AC-7)

Tandem Mapping

Tandem Policies

- Access Control
- Personnel Security
- Remote Access
- Remote Work
- User Authentication

Tandem Risk Assessment Controls

- Limit Local Administrator Access
- Logical Access Controls
- Physical Access Controls

Tandem Blog

- What is Multifactor Authentication?
- The Challenges of Multifactor Authentication

Access Control

AUTHENTICATION REQUIREMENTS & GUIDELINES

Checklist

- [ ] Require employees to authenticate to access systems.
- [ ] Have and enforce minimum guidelines for things like:
  - Password complexity.
  - Password reuse.
  - Password age.

Resources

FFIEC Authentication and Access to Financial Institution Services and Systems Guidance

NIST Cybersecurity Framework: PR.AC-1, PR.AC-6, PR.AC-7

Tandem Mapping

Tandem Policies: User Authentication

Tandem Risk Assessment Controls

- Logical Access Controls

FREDDIE MAC GUIDE 1302.2(b)(xvii)(C)

Authentication requirements and guidelines

Seller/Servicers must require employees to authenticate or prove their identity to the system through a private, protected method or process that includes, but is not limited to, user identification codes, passwords, personal identification numbers, a smart card and/or a token device. If passwords are used, the Authentication policy must mandate, and Seller/Servicers must enforce, minimum guidelines for password complexity, reuse timelines and password change timelines.

DID YOU KNOW?

98.6% of financial institutions say their access controls include password complexity and limits to password attempts and reuse.

Source: Tandem Cybersecurity Assessment Tool Peer Analysis (04/2023)

FREDDIE MAC GUIDE 1302.2(b)(xvii)(D)

Asset management

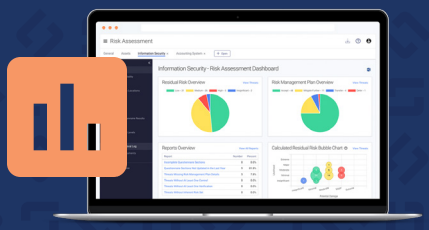
Seller/Servicers must maintain an inventory management system to track physical and software assets, such as end-user technology, servers, network devices, and corresponding asset ownership. The inventory management system must be reconciled to actual inventory at least annually to verify all assets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

Documented procedures must be in place detailing guidelines and requirements for tracking the removal of assets from a facility.

PRODUCT SPOTLIGHT

Tandem Risk Assessment features an IT asset management component, designed to help you maintain an inventory of your information assets.

See how Tandem can improve your IT asset management practices at Tandem.App/Information-Security-Risk-Assessment-Software.



Checklist

- [ ] Have an IT asset inventory.
- [ ] Ensure the inventory addresses things like:
  - Workstations
  - Mobile devices
  - Servers
  - Network devices (e.g., routers, switches, etc.)
  - Ownership / responsibility
- [ ] Reconcile the IT asset inventory with the actual inventory at least annually.
- [ ] Document procedures for the secure disposal of assets.

Resources

FFIEC Information Security Booklet

- Section II.C.5 Inventory and Classification of Assets
- Section II.C.13(c) Disposal of Information

FFIEC Architecture, Infrastructure, and Operations Booklet

- III.B IT Asset Management

FFIEC Authentication and Access to Financial Institution Services and Systems Guidance

NIST Cybersecurity Framework: ID.AM-1, ID.AM-2, PR.DS-3

Tandem Mapping

Tandem Policies: IT Asset Management

Tandem Risk Assessment: Asset Management

Access Control

CLOUD COMPUTING

Checklist

- [ ] Have a written cloud computing policy.
- [ ] Get it approved by management.
- [ ] Communicate it with appropriate personnel.
- [ ] Review the policy on a regular basis.

Resources

FFIEC Information Security Booklet

- Section II.C.20(a) Outsourced Cloud Computing

FFIEC Architecture, Infrastructure, and Operations Booklet

- VII.A Cloud Computing

FFIEC Outsourcing Technology Services Booklet

FFIEC Joint Statement Security in a Cloud Computing Environment

Tandem Mapping

Tandem Policies: Cloud Computing

Tandem Blog

- What is Vendor Management?
- 4 Steps to Simplify Your Vendor Due Diligence Process
- Review Your Vendor's SOC Report (SSAE 18) in 15 Minutes

FREDDIE MAC GUIDE 1302.2(b)(xvii)(E)

Cloud computing

When a Seller/Servicer consumes or provides cloud services that store, process, access or transmit Freddie Mac confidential information or Protected Information or connect to any System, the Seller/Servicer must maintain a formal cloud computing policy that has been approved by management and communicated to appropriate personnel, and the Seller/servicer must designate an owner to maintain and review the policy to ensure it consistently reflects industry best practices.

TRIVIA ANSWER

(See Page 6 for the question!)

There are currently 10 booklets in the FFIEC IT Examination Handbook.

- Architecture, Infrastructure, and Operations (AIO)
- Audit (AUD)
- Business Continuity Management (BCM)
- Development and Acquisition (D&A)
- Information Security (IS)
- Management (MGT)
- Outsourcing Technology Services (OTS)
- Retail Payment Systems (RPS)
- Supervision of Technology Service Providers (TSP)
- Wholesale Payment Systems (WPS)

The topic of cloud computing is most thoroughly addressed in the AIO booklet.

Access Control

VENDOR RISK MANAGEMENT PROGRAM

FREDDIE MAC GUIDE 1302.2(b)(xvii)(F)

Vendor risk management program

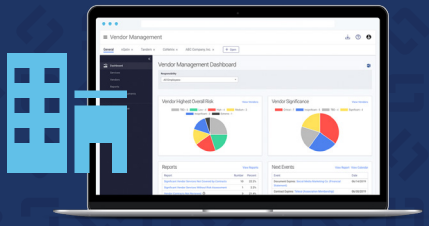
Seller/Servicers must implement a vendor risk management program to formally evaluate, track and measure third-party risk; to assess its impact on all aspects of the organization's business; and to develop compensating controls or other forms of mitigation to safeguard and protect Freddie Mac confidential information and Protected Information from unauthorized persons, malicious software or other harmful computer information, commands, codes or programs.

Seller/Servicers must maintain with all Related Third Parties that store, process, access or transmit Freddie Mac confidential information or Protected Information a written agreement that obligates them to comply with Minimum Requirements similar to what is outlined within this chapter.

PRODUCT SPOTLIGHT

Tandem Vendor Management is designed to help you oversee and manage your third-party risk. This product's streamlined interface is designed to organize your vendor management program, including vendor risk assessments, contract management, due diligence documents, reviews, and more.

See how Tandem can improve your vendor oversight practices at Tandem.App/Vendor-Management-Software.



Checklist

- ☐ Implement a vendor management program.
- ☐ Formally evaluate, track, and measure third-party risk.
- ☐ Assess the vendor's impact on your business.
- ☐ Implement controls to protect confidential data stored, processed, and/or accessed by the vendor.
- ☐ Have a written agreement with third parties that store, process, or transmit confidential information that requires them to implement appropriate information security measures.

Resources

FFIEC Information Security Booklet

- Section II.C.20 Oversight of Third-Party Service Providers
- Section II.C.14 Supply Chain
- Section II.C.17 Application Security

FFIEC Architecture, Infrastructure, and Operations Booklet

- III.E Oversight of Third-Party Service Providers

FFIEC Business Continuity Management Booklet

- IV.A.5 Third-Party Service Providers

FFIEC Outsourcing Technology Services Booklet

Federal Agency Guidance

- FDIC FIL 44-2008 Guidance for Managing Third-Party Risk
- FRB 13-19 Guidance on Managing Outsourcing Risk
- OCC Bulletin 2013-29 Third-Party Relationships: Risk Management
- OCC Bulletin 2020-10 Third-Party Relationships: FAQ
- NCUA SL 07-01 Evaluating Third Party Relationships

NIST Cybersecurity Framework: ID.SC-2, ID.SC-3, ID.SC-4

Tandem Mapping

Tandem Vendor Management

Tandem Policies: Vendor Management

Privacy Incident Requirements

Checklist

- [ ] Email Freddie Mac ASAP and within 48 hours of discovery (privacy_incident_management@freddiemac.com).
- [ ] Include the following information (as applicable):
  - The name, phone number, and email of the lead incident handler.
  - Internal and external investigations.
  - Point of contact information for the Seller/Servicer.
  - Law enforcement agencies involved.
  - All known details.
- [ ] Analyze, contain, and eradicate the incident ASAP.
- [ ] Identify confidential information affected by the incident.
- [ ] Comply with other notification laws.
- [ ] Allow Freddie Mac to review and comment on any notifications which may be sent to borrowers, if Freddie Mac will be referenced.
- [ ] Provide Freddie Mac with any and all information they request, in case they have to make their own statement on the issue.
- [ ] Provide technical and forensic reports to Freddie Mac as available.

Resources

FFIEC Information Security Booklet

- Section III.C Incident Identification and Assessment
- Section III.D Incident Response

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section VI.C.4 Event, Incident, and Problem Management

FFIEC Business Continuity Management Booklet

- V.F.1 Incident Response

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide

NIST Cybersecurity Framework: PR.IP-9, RS.RP-1, RS.CO-2, RS.AN-2, RS.MI-1, RS.MI-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3

FREDDIE MAC GUIDE 1302.2(b)(xviii)

Privacy Incident Requirements

Excepting only Non-critical Privacy Events for which there is a different reporting requirement (as defined and described below), [the Seller/Servicer must] notify Freddie Mac via e-mail at Privacy_Incident_Management@FreddieMac.com as soon as possible, but no later than 48 hours after discovering the Privacy Incident.

Thereafter:

A. Provide the name, phone number and e-mail address of the contact leading the Privacy Incident investigation.

B. Promptly investigate, correct and mitigate the Privacy Incident at the Seller/Servicer's expense, including identifying all Freddie Mac confidential information or Protected Information affected by the Privacy Incident and preventing the continuation and recurrence of the Privacy Incident.

C. Comply in a timely manner with Applicable Laws (as defined in Section 1301.2) concerning notification requirements, giving Freddie Mac the opportunity to first review and comment on any notifications to Borrowers (if Freddie Mac is directly or indirectly identified in such notifications) or to regulatory or other State offices.

D. Promptly following a request by Freddie Mac, provide Freddie Mac and its designees all information and assistance needed to enable Freddie Mac to evaluate the need for, and to timely make, any notification it deems necessary or advisable concerning the Privacy Incident.

E. Provide Freddie Mac with such information, including technical and forensic reports if available, as Freddie Mac may reasonably request to assist Freddie Mac in evaluating the effect of the Privacy Incident on Freddie Mac's infrastructure and impacted Borrowers or employees. Within 48 hours after discovering the Privacy Incident, and thereafter as requested, provide Freddie Mac via e-mail at Privacy_Incident_Management@FreddieMac.com (or by such other means as Freddie Mac may otherwise request) all known details of the Privacy Incident, including related internal and external investigations and point of contact information for the Seller/Servicer and any law enforcement agencies involved for further inquiries.

Privacy Incident Requirements

FREDDIE MAC GUIDE 1302.2(b)(xviii)

Privacy Incident Requirements (cont'd)

Ongoing reporting requirements in the event of a Privacy Incident – Seller/Servicer must report to Freddie Mac at Privacy_Incident_Management@FreddieMac.com (or by such other means as Freddie Mac may otherwise request), and provide the following information:

A. Details and information as to the nature and impact of the Privacy Incident on Freddie Mac confidential information or Protected Information;

B. The nature and details of the information accessed, taken or exposed;

C. The likelihood of misuse and all facts and information relevant to actual or potential misuse;

D. All risk factors and potential damage estimates associated with the Privacy Incident (including reputational risk);

E. All actions that are being and will be taken to remediate the Privacy Incident and its cause, to protect individuals, business assets and Freddie Mac confidential information and Protected Information in the future, and to comply with Applicable Laws;

F. All postmortem and similar after-action reports generated; and

G. As and when requested by Freddie Mac, any other details and information concerning the Privacy Incident (e.g., final incident closure report, Certificate of Compliance (in form and substance requested by Freddie Mac evidencing, among other things, that the Seller/Servicer has, with respect to the Privacy Incident, complied with applicable federal, State and local data breach notification laws and regulations and the Guide), details such as causation factors and remediation actions or workarounds and lessons learned from the incident) and copies of any communications to Borrowers, State and federal agencies and offices, regulators, credit reporting agencies or others, and any interim status updates Freddie Mac may request, including details on information gained and progress made since the last update, until Freddie Mac is satisfied that there has been compliance with Applicable Laws and the event giving rise to the Privacy Incident is fully resolved and closed.

Checklist

As the incident response process continues, provide details about:

- ☐ The nature and impact of the incident on confidential information.
- ☐ The nature and details of information accessed, taken, or exposed.
- ☐ The likelihood of misuse and relevant evidence.
- ☐ The risk factors and potential damage estimates.
- ☐ The actions taken to respond, remediate, and prevent recurrence.
- ☐ The postmortem and after-action reports.
- ☐ Anything else Freddie Mac requests to verify the incident is resolved.

FREE RESOURCE

Incident Tracking Form

If you had a security or privacy incident, where would you start?

Walk through the six-stages of incident response, recommended by NIST, using this fillable incident tracking form. This free resource was designed to help organizations, like yours, make sure that if you have an incident, your bases are covered.

See how Tandem can help you.

Tandem.App/Incident-Tracking-Form


Incident Tracking Form

GENERAL INFORMATION

Complete the following fields to document general information about the incident.

Incident Name | Reported By

Occurrence Date & Time | Reported Date & Time | Email Address

Status | Phone Number

Summary

HANDLERS

Document the names and contact information of the individuals responsible for managing the incident.

Lead Incident Handler | Public Relations Coordinator

Technical Specialist | Audit & Compliance Specialist

Legal Advisor | Other Handlers

Visit Tandem.App for more incident management resources.
Tandem, LLC Copyright © 2021

Privacy Incident Requirements

Checklist

For non-critical privacy incidents affecting 10 or fewer borrowers:

- ☐ Respond in accordance with all applicable laws.
- ☐ Report these non-critical incidents to Freddie Mac quarterly (i.e., by the 15th day of January, April, July, and October).
- ☐ If any of the following circumstances apply, regardless of the number of borrowers affected, the 48-hour rule applies.

  - A malicious actor caused the breach
  - The exposure has or will result in misuse of breached data.
  - The breach is required to be reported by state laws.
  - There is active or expected media coverage.
  - Law enforcement has been or will be involved.
  - A regulator sends a notice of non-compliance.
  - There is a material risk to borrowers, investors, Freddie Mac, or others.

Tandem Mapping

Tandem Incident Management

Tandem Policies: Incident Management

Tandem Blog: Incident Response Plan Communication Guidelines

PRODUCT SPOTLIGHT

Incident Management

Put your organization ahead of the curve by creating a plan for handling incidents. When an incident occurs, track and document the response process through the six stages outlined by the National Institute of Standards and Technology (NIST SP800-61 Rev. 2). Learn more at Tandem.App/Incident-Management-Software.

FREDDIE MAC GUIDE 1302.2(b)(xviii)

Privacy Incident Requirements (cont'd)

If a Privacy Incident affects ten or fewer Freddie Mac Borrowers ("Non-critical Privacy Events"), a Seller/Servicer is required to respond to the Privacy Incident in accordance with all Applicable Laws, but a Seller/Servicer is not required to report such Non-critical Privacy Events to Freddie Mac within the 48-hour reporting window referenced above.

Seller/Servicers must report Non-critical Privacy Events to Freddie Mac on a quarterly basis. Seller/Servicers must submit such reports to Freddie Mac by the 15th day of each January, April, July and October, in each case covering Non-critical Privacy Events in the three immediately preceding calendar months.

For clarity and notwithstanding the exception for Non-critical Privacy Events, if a Privacy Incident involves any of the issues listed below, a Seller/Servicer must report the Privacy Incident to Freddie Mac within 48 hours (in accordance with this Section 1302.2) and comply with this Section 1302.2, regardless of the number of impacted individuals:

- A malicious actor caused the breach;
- There is suspicion or confirmation that the exposure has led or will lead to improper use of the breached data;
- The impacted States/territories or federal statute require the Seller/Servicers to notify State or federal regulators;
- There is active or anticipated media coverage of the Privacy Incident;
- Law enforcement has been or will be contacted regarding the Privacy Incident;
- The Seller/Servicer receives notice from a regulator that it is not or may not be compliant with its breach response obligations; or
- The Seller/Servicer is aware of or reasonably should anticipate material risk to Borrowers, investors, Freddie Mac (including without limitation, Freddie Mac's infrastructure or its reputation) or others, based on specific facts and circumstances.

Security Incident Requirements

FREDDIE MAC GUIDE 1302.2(b)(xviii)

Security Incident Requirements

As soon as possible, but no later than 48 hours after discovering the Security Incident, notify Freddie Mac via e-mail at Information_Security@FreddieMac.com of the Security Incident. Thereafter, the Seller/Servicer must:

A. Provide the name, phone number and e-mail address of the contact leading the Security Incident investigation.

B. Promptly investigate, correct and mitigate the Security Incident at the Seller/Servicer's expense, including identifying all Freddie Mac confidential information or Protected Information affected by the Security Incident and preventing the continuation and recurrence of the Security Incident.

C. Comply in a timely manner with Applicable Laws (as defined in Section 1301.2) concerning notification requirements, first giving Freddie Mac the opportunity to review and comment on any notification that in any way refers to or identifies Freddie Mac. Promptly following a request by Freddie Mac, provide Freddie Mac and its designees all information and assistance needed to enable Freddie Mac to timely make any notification it deems necessary or advisable concerning the Security Incident.

D. Provide Freddie Mac with such information, including technical and forensic reports, as Freddie Mac may reasonably request to assist Freddie Mac in evaluating the effect of the Security Incident on Freddie Mac, Freddie Mac confidential information, Protected Information, Freddie Mac's operations and impacted Borrowers.

E. Within 48 hours after discovering the Security Incident, and thereafter as requested, provide Freddie Mac via e-mail at Information_Security@FreddieMac.com (or by such other means as Freddie Mac may otherwise request) all known details of the Security Incident, including related internal and external investigations and technical indicators of compromise (e-mail addresses, hash values, IP addresses, malware code, vector of compromise, etc.), all tactics, techniques, and procedures associated with the incident, details surrounding the attack methodology and timing of the incident, and point of contact information for the Seller/Servicer and any law enforcement agencies involved for further inquiries.

Checklist

- ☐ Email Freddie Mac ASAP and within 48 hours of discovery (information_security@freddiemac.com).
- ☐ Include the following information (as it becomes available):
  - The name, phone number, and email of the lead incident handler.
  - Internal and external investigations.
  - Technical indicators of compromise (e.g., email addresses, hash values, IP addresses, malicious code, compromise vectors, etc.).
  - All associated tactics, techniques, and procedures.
  - Timing and methodology details.
  - Point of contact information for the Seller/Servicer.
  - Law enforcement agencies involved.
  - All other known details.
- ☐ Analyze, contain, and eradicate the incident ASAP.
- ☐ Identify confidential information affected by the incident.
- ☐ Comply with other notification laws.
- ☐ Allow Freddie Mac to review and comment on any notifications which may be sent to borrowers, if Freddie Mac will be referenced.
- ☐ Provide Freddie Mac with any and all information they request, in case they have to make their own statement on the issue.
- ☐ Provide technical and forensic reports to Freddie Mac as available.

Resources

FFIEC Information Security Booklet

- Section III.C Incident Identification and Assessment
- Section III.D Incident Response

FFIEC Architecture, Infrastructure, and Operations Booklet

- Section VI.C.4 Event, Incident, and Problem Management

FFIEC Business Continuity Management Booklet

- V.F.1 Incident Response

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide

NIST Cybersecurity Framework: PR.IP-9, RS.RP-1, RS.CO-2, RS.AN-2, RS.MI-1, RS.MI-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3

Security Incident Requirements

Checklist

As the incident response process continues, provide details about:

- [ ] If and what confidential information was accessed, taken, or exposed.
- [ ] The nature of information accessed, taken, or exposed.
- [ ] The likelihood of misuse and relevant evidence.
- [ ] Potential damage estimates (including reputation risk).
- [ ] The actions taken to remediate, identify the root cause, and prevent recurrence.
- [ ] The postmortem and after-action reports.

When requested, provide the following to Freddie Mac:

- [ ] Final incident closure report.
- [ ] Remediation actions, workarounds, and corrections.
- [ ] Eradication and recovery steps taken.
- [ ] Lessons learned.
- [ ] Copies of communications to borrowers, state and federal agencies, regulators, credit reporting agencies, etc.
- [ ] Interim status updates on information gained and progress made since the last update.
- [ ] Anything else Freddie Mac requests to verify the incident is resolved.

Tandem Mapping

Tandem Incident Management

Tandem Blog

- 6 Phases of an Effective Incident Response Plan
- Incident Response Plan Communication Guidelines
- Ransomware Incident Response Playbook
- Security Incident Management Training: What Employees Need to Know
- Third-Party Incident Response Playbook
- Your Financial Institution Incident Management Guidance Cheat Sheet

FREDDIE MAC GUIDE 1302.2(b)(xviii)

Security Incident Requirements (cont'd)

Ongoing reporting requirements in the event of a Security Incident – Seller/Servicers must report to Freddie Mac at Information_Security@FreddieMac.com (or by such other means as Freddie Mac may otherwise request):

A. Details and information as to whether, and if so the extent to which, Freddie Mac data was accessed, taken or exposed;

B. The nature of the information accessed, taken or exposed;

C. The likelihood of misuse of the information and, if applicable, how the information was misused;

D. Any potential damage estimates associated with the Security Incident (including reputational risk);

E. All actions that are being taken to remediate the Security Incident and its cause and to protect individuals and business assets in the future; and

F. Any resulting after-action reports generated

1302.2(b)(xviii)

Security Incident Requirements (cont'd)

Provide to Freddie Mac, as and when requested, other details concerning the Security Incident (final incident closure report, details such as remediation actions, workarounds or corrections that resolved the incident and restored service to its best quality, eradication and recovery steps taken, and lessons learned from the Security Incident) and copies of any communications to Borrowers, State and federal agencies, regulators, credit reporting agencies or others, as well as any interim status updates Freddie Mac may request, including details on information gained and progress made since the last update, until Freddie Mac is satisfied that the event giving rise to the Security Incident is fully resolved and closed.

If a provision of the Guide or a Seller/Servicer's other Purchase Documents require more stringent Minimum Requirements or reporting of Security Incidents or Privacy Incidents, then the Seller/Servicer must adhere to those more stringent requirements.

About Tandem

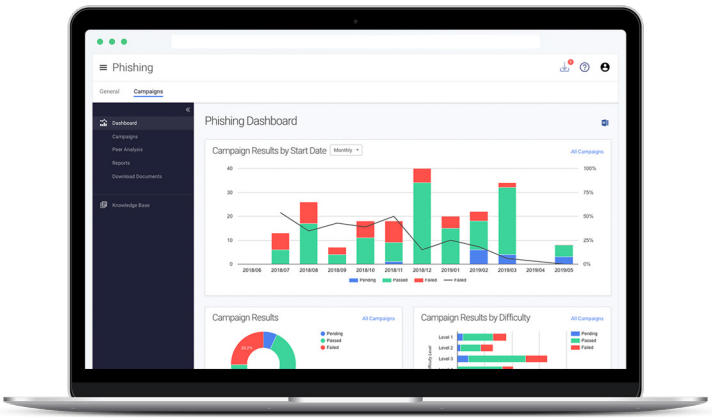
WHO WE ARE

Tandem, LLC is owned by CoNetrix, LLC, along with Tandem's sister companies, CoNetrix Technology and CoNetrix Security. Tandem is a software-as-a-service created to ease the burden of information security compliance for the financial institution industry.

Tandem first started out by helping our clients maintain their documents, but it didn't take long to decide that a software solution could help more people, faster. In 2007, we began developing the do-it-yourself compliance application for information security, now known as Tandem.

We named our product Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs. We bring software built by information security experts to help you create, organize, and manage your information security program.

We believe you have what it takes to manage information security and regulatory compliance. With the right tool, you can do it fast. Learn more about how Tandem can help you at Tandem.App.



OUR PRODUCTS

- Audit Management
- Business Continuity Plan
- Compliance Management
- Cybersecurity
- Identity Theft Prevention
- Incident Management
- Internet Banking Security
- Phishing
- Policies
- Risk Assessment
- Vendor Management

info@tandem.app
844-698-9800