March 1, 2023

Information Security and Privacy Updates

Guide Bulletin 2023-6 includes the most recent updates to Guide Chapter 1302 effective **July 3, 2023**. This chapter contains the minimum information security program requirements that Seller/Servicers must implement within their systems to reduce the impact and likelihood of unauthorized persons (or authorized person(s)) with malicious or unlawful intentions from gaining access to Freddie Mac proprietary information, data and consumer personal non-public information.

This side-by-side comparison is not a replacement or substitute for reviewing the requirements found in the Guide or other Purchase Documents. It's intended solely to illustrate at a high level various revisions pertaining to information security, privacy and third-party risk requirements.

It's important for Seller/Servicers to initiate their own impact assessment as quickly as possible, as the new requirements will have varying levels of impact depending on their current information security and privacy infrastructure and business processes. For questions or more information, please reach out to your Freddie Mac representative or the Customer Support Contact Center (800-FREDDIE).

GUIDE SECTION	CURRENT REQUIREMENT	NEW/UPDATED REQUIREMENT
Section 1302.1 **Overview of information security and business continuity planning requirements**	This Section provides an overview of Freddie Mac information security and business continuity planning Minimum Requirements.	New requirements include: • Seller/Servicers' information security program and business continuity plan requirements must include the confidentiality, integrity and availability of Freddie Mac confidential information and Protected Information retained by the Seller/Servicer following Freddie Mac termination of the Seller/Servicers' right to sell or service mortgages. • Seller/Servicers' failure to comply with the Minimum Requirements for information security and business continuity included in this Chapter 1302 may result in the termination of a Seller/Servicer's access to any or all Freddie Mac Systems.
Section 1302.2(a) **Relevant terms**	Relevant terms are: • Authentication • Encryption	'Vulnerability management' has been added as a relevant term.
Section 1302.2(b)(i) **Information security program**	Seller/Servicers are required to have written minimum security standards that include user responsibilities, ownership of information, baseline security practices, technical security protection mechanisms and other requirements.	We've added specificity to the existing requirements as follows: • A Seller/Servicer must define a group or individual responsible for development of information security requirements, including the adoption, implementation, maintenance and administration of the written minimum security standards, policies, and procedures.

	Seller/Servicers are required to review their information security policies and procedures used in connection with the selling and servicing of Freddie Mac mortgages at least annually, to ensure compliance with the Guide and other Purchase Documents.	• **Not less than annually**, Seller/Servicers must review and assess the adequacy of their information security policies and procedures to ensure compliance with the Guide, other Purchase Documents, and industry best practices including as set forth by the FFEIC and NIST. • Upon request by Freddie Mac, a Seller/Servicer must provide an attestation of the adequacy of its information security policies and procedures. Attestation may be requested even after Freddie Mac terminates a Seller/Servicer's right to sell or service mortgages.
Section 1302.2(b)(ii) **Human resources security**	Seller/Servicers are required to conduct pre-employment screening and background verification checks for all candidates for employment, including contractors. Information security awareness training is required for all employees and relevant contractors and third parties.	Prior to being granted access to Freddie Mac confidential information, Protected Information or Systems, Seller/Servicers must require all employees, contractor personnel and third parties to either sign a non-disclosure agreement **or** be subject to a code of conduct that includes obligations to restrict use, disclosure, and maintain as confidential such information.
Section 1302.2 (b)(iii) **Physical and environmental security controls**	Seller/Servicers are required to create and maintain a physical security control program of the organization's buildings and facilities and have environmental controls to protect from loss of connectivity, or damage from natural or man-made disasters and adverse events.	We've added language to provide greater clarity on existing requirements. Seller/Servicers are now required to maintain "an updated list of personnel with authorized access to facilities where information systems reside" and to perform an access privilege review **at least annually**, as well as upon departure of authorized personnel.
Section 1302.2 (b)(iv) **Communications and operations management**	Seller/Servicers must implement technical security measures to monitor for malicious software, stop unwanted spam traffic and protect against unauthorized wireless connections.	The updated requirements bolster the technical security measures, including requiring that the measures should *monitor for, mitigate against, and prevent* malicious software.

Section 1302.2 (b)(v)
Old Title:
Removable media policy
New Title:
Data transmission and data loss prevention
	Seller/Servicers are required to restrict the transfer of data to USB and other removeable media to only personnel with a business need for the removeable media to complete their activities. If removeable media is used, it must be logged on an exception basis, listing the user and business case, and the media must be encrypted.	In addition to the current requirements, Seller/Servicers must:
		• Have in place a data loss prevention/transmission protection mechanism and implement a written policy establishing requirements to protect confidentiality and integrity of information exchange using technology applications or information systems.
		• Ensure adequate and up-to-date loss prevention software is used and a process is in place to:
		  ○ Scan for sensitive info stored on disk and outgoing transmissions over public communication paths, and
		  ○ Restrict the transfer of data to removeable media devices.

Section 1302.2 (b)(vii) Old Title: **Boundary protection** New Title: **Network security**	Seller/Servicers are required to implement information technology controls such as firewalls, and restrict all ports, protocols, and services to those required for business operations.	In addition to greater specificity to the current requirements, Seller/Servicers will be required to formally recertify and authorize the organization's firewall rules **upon each significant change in infrastructure, or not less than annually**.
Section 1302.2 (b)(viii) NEW: **Mobile computing**	There is no current requirement.	Seller/Servicers must have a written mobile device/computing management (MDM) policy that reflects current best practices covering, but not limited to the following areas: • Approved and prohibited application • Cryptogenic mechanisms to ensure data security • Identity and access management • Software updates
Section 1302.2 (b)(ix) **Wireless networks**	Seller/Servicers are required to control, secure and monitor wireless access points, and if supporting wireless network users, also implement strong WLAN authentication, prohibit use of WEP algorithm, validate and verify authorized users and access points, and ensure the administrator access to the router is password protected.	We've added specificity related to access controls and information security, including requiring that **at least annually**, Seller/Servicers perform reviews of approved wireless networks to validate and verify authorized users and access points.
Section 1302.2 (b)(x) **Vulnerability management**	Seller/Servicers are required to conduct vulnerability testing on a regular basis and have a process in place to analyze and remediate identified vulnerabilities.	In addition to current requirements, Seller/Servicers must: • Employ a qualified independent third-party to conduct penetration testing, **no less than annually**. • Develop and implement a vulnerability assessment process and policy with a designated owner and conduct the assessment **at least annually**. • Remediate all identified vulnerabilities and maintain a record of all identified vulnerabilities with their status and associated remediation plan.
Section 1302.2 (b)(xi) **Configuration and patch management**	Seller/Servicers are required to: • Have a process for developing and maintaining secure	We've added specificity to current requirements.

	configuration baselines of infrastructure components. • Deploy an intrusion detection and prevention system that feeds event information to centralized systems for analysis. • Define preventive controls to block malicious messages and attachments from entering the environment. • Identify a group responsible for software updates and patches.	Seller/Servicers must implement a management-approved patch management process and designate an owner who maintains and reviews the policy to ensure it consistently reflects industry best practices.
Section 1302.2 (b)(xii) NEW: **Auditing, logging and monitoring**	There is no current requirement.	• Seller/Servicers are required to implement a process for logging and monitoring activities within information systems, including integration with the company's enterprise log management function, if applicable. • This process should include requirements for log retention and handling to ensure logs retain relevant, useable, and timely information sufficient to identify significant user access and/or system activities. • The control environment must undergo an independent security **assessment not less than annually and in the event of any data security or privacy incident as defined in the Guide**.
Section 1302.2 (b)(xiii) NEW: **Software and application development life cycle (SDLC)**	There is no current requirement.	Seller/Servicers that develop applications or software to store, access, process or transmit Freddie Mac information, or connect to Freddie Mac Systems, are required to implement a written software and application development lifecycle (SDLC) process and policy that meets, at least, the requirements prescribed in the Guide, including: • Separation of production and development environments • Secure coding requirements • Open-source requirements • Code development and scanning pre- and post-deployment
Section 1302.2 (b)(xiv) **Data encryption**	Seller/Servicers are required to use encryption during transmission of any sensitive data, and portable end-user devices must be equipped with encryption mechanisms that protect data in case the device is lost or stolen.	In addition to added specificity to existing requirements, Seller/Servicers are required to: • Implement a formal encryption and cryptography use policy that is management approved and administered to ensure industry best practices. • Ensure the policy meets or exceeds then-current industry standards and prohibits use of outdated technology.

Section 1302.2 (b)(xv) NEW: **Incident management**	There is no current requirement.	Seller/Servicers must develop an incident response plan that includes a roadmap for implementing incident response capabilities and defines the resources and management support needed. The incident response plan/capabilities must be tested **at least annually** unless the plan has been formally activated.
Section 1302.2 (b)(xvii)(A) **Access control: Access management policy**	Seller/Servicers are required to • Establish an access management policy that includes a process for granting and removing system access, requirements for authentication, and rules of behavior. • Define remote access requirements. • Define access and authentication requirements for system administrators including enforcing 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 multi-factor authentication where applicable. • Monitor user accounts for users of any Freddie Mac systems who no longer need access due to job change or termination, and notify Freddie Mac within one business day of, or prior to, a transfer or termination.	In addition to adding specificity to existing requirements, Seller/Servicers must: • Define and enforce access and authentication requirements for system administrators and other privileged accounts. • Define and enforce requirements around locked accounts. • Refer to and comply with the instructions to update systems access for relevant applications at https://sf.freddiemac.com/tools-learning/technology-login • Seller/Servicers must now notify Freddie Mac within 24 hours of, or prior to, a transfer or termination of anyone with user account access to Freddie Mac systems.
Section 1302.2 (b)(xvii)(B) **Access control: Granting, removing and reviewing access**	Seller/Servicers must maintain written procedures for: • Approval of access requests • Removal of access for terminations • Periodic account maintenance and reconciliation	Seller/Servicers must: • **At least annually,** review all user access privileges and certify access according to minimum information necessary rules. • Prohibit or prevent using the same service account identifiers and passwords in production and non-production environments.

Section 1302.2 (b)(xvii)(C) **Access control: 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 which includes, but is not limited to, user ID codes, passwords, personal ID numbers, a smart card and or a token device. If passwords are used, the policy must mandate minimum guidelines for password complexity, reuse timelines, and password change timelines.	If password access is used, Seller/Servicers must *enforce*, as well as mandate, minimum guidelines for password complexity, reuse timelines and password change timelines.
Section 1302.2 (b)(xvii)(D) **Access control: Asset management**	Seller/Servicers must maintain an inventory management system to track physical and software assets, and the inventory management system must be reconciled to actual **inventory on a periodic basis**.	A Seller/Servicer's inventory management system must be reconciled to actual inventory **at least annually**.
Section 1302.2 (b)(xvii)(E) NEW: **Access control: Cloud computing**	There is no current requirement.	If cloud services are used for Freddie Mac confidential information or Protected Information, or connect to any Freddie Mac System, Seller/Servicers must have a formal management-approved cloud computing policy, with an individual who is responsible for maintaining and reviewing the policy to ensure it reflects industry best practices.
Section 1302.2 (b)(xvii)(F) **Access control: Vendor risk management program**	Seller/Servicers must: • Implement a vendor risk management program that evaluates, tracks and measures third-party risk, and assesses its impact on aspects of the organization's business • Develop compensating controls to protect Freddie Mac information from unauthorized persons, malicious software, etc.	In addition to current requirements, Seller/Servicers must: • Have a written agreement in place with all Related Third Parties that outlines the Minimum Requirements associated with storing, processing, accessing, or transmitting Freddie Mac confidential information and Protected Information.
Section 1302.2 (b)(xviii) Old title: **Incident notification and related obligations** New title: **Breach notification and related obligations**	If a Seller/Servicer knows or believes there has been unauthorized acquisition of data or computing resources, or unauthorized access to data, the Seller/Servicer must follow the requirements in the Security Incident requirements included with this Section of the Guide.	With this update, the Guide further differentiates a Security Incident from a Privacy Incident and provides reporting requirements for each; there is also a new carve out for less frequent reporting of non-Critical Privacy Incidents detailed below. There are new e-mail mailboxes for reporting Security Incidents and Privacy Incidents. (See the tables in Guide Section 1302.2 (b)(xviii) for precise requirements.) **Privacy Incidents**

		• 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 Freddie Mac confidential information or Protected Information has been exposed, accessed, or used without authorization, it must be **reported as soon as possible, but no later than within 48 hours of discovering the incident**. • Report a Privacy Incident to Freddie Mac via email: **Privacy_Incident_Management@FreddieMac.com** • If a Privacy Incident involves any of the following issues, the Non-critical Privacy Incident reporting exception noted below does not apply, and reporting **within 48 hours of discovery** is required if: ○ A malicious actor caused a breach ○ Suspicion or confirmation that the exposure has or will lead to improper use of the breached data ○ Impacted statutes require the Seller/Servicers to notify State or federal regulators ○ There is active or anticipated media coverage of the incident ○ Law enforcement is or will be contacted regard the incident ○ Seller/Servicer receives notice from a regulator that it is or may not be compliant with its breach response obligations ○ Seller/Servicer is aware of or reasonable should anticipate a material risk to borrowers, investors, Freddie Mac or others • Freddie Mac considers a Privacy Incident affecting ten or fewer Freddie Mac borrowers as a "Non-critical Privacy Event" and Seller/Servicers are required to report these incidents on a quarterly schedule (January 15, April 15, July 15 and October 15), rather than **within 48 hours of discovery**. *Note: The Guide does not yet provide a form for reporting Non-critical Privacy Events. We are working to finalize that form and will publish the information and tools needed to meet this requirement in an upcoming Bulletin.* **Security Incidents** • Report a Security Incident to Freddie Mac via email to: **Information_Security@FreddieMac.com** as soon as possible but not later than **within 48 hours of discovering the incident**.

		• Submit ongoing reporting and other details to Freddie Mac by providing the information outlined in the Security Incident requirements table in the Guide.
Section 1302.3 Business continuity planning	Seller/Servicers are required to: • Have a business continuity plan in place that addresses potential disruptions and is reviewed and updated annually. • Establish a governing body to provide guidance for the plan. • At least annually conduct a business disruption analysis and test the plan, including the recovery of predefined critical business function. • Conduct a formal risk assessment of the organization at least once every two years or more frequently if there are significant changes. • Establish a formal crisis management team with responsibility for declaring a crisis and implementing a documented crisis management plan. • Establish a documented crisis management plan that is reviewed and updated annually. • Require any related third party to comply with requirements in Guide Section 1302.2 and Section 1302.3, and to refrain from interfering with any obligations the Seller/Servicer may have to Freddie Mac. • Designate Freddie Mac as an express, intended third-party beneficiary of each agreement with a related third party. • Indemnify Freddie Mac from all liabilities arising directly or indirectly out of damages caused by any breach of a Seller/Servicer or related third party.	In addition to adding specificity to existing requirements, the new requirements include: • A Seller/Servicer must be able to maintain and restore retained information, including following Freddie Mac's termination of Seller/Servicer's right to sell or service mortgages, unless appropriate due diligence has been performed permitting the destruction of such information, and the information destruction requirements have been met. • When electronic information is destroyed, Seller/Servicers must ensure it is rendered unreadable and incapable of being re-created. • Hard copy records must be properly and securely destroyed and must be accompanied by a certificate of destruction. • Upon request, Seller/Servicer will provide Freddie Mac certificates of destruction or other evidence demonstrating the fact and manner of destruction, be it electronic, paper, hard drive, or other media that contained the subject information. • Seller/Servicers must provide their documented crisis management plan to Freddie Mac upon written request. • Designation of Freddie Mac as an express, intended third-party beneficiary of each Related Third Party agreement is not required for agreements with Seller/Servicer's counterparties who also have direct relationship(s) with Freddie Mac relative to the same subject matter. For example, mortgage insurance companies, credit bureaus or warehouse lenders. *Note: The Guide does not yet provide the protocol for obtaining information on direct relationships Freddie Mac may have with third parties. We are working to finalize that process and will publish additional information in an upcoming Bulletin.*