INFORMATION SECURITY

Compliance Requirements

Fannie Mae
Freddie Mac
State & Federal Agencies

HOUSING RESEARCH PRESS

ACKNOWLEGEMENT

Sources used in the preparation of this material include the following agencies and organizations:

CONFERENCE OF STATE BANK SUPERVISORS (CSBS)

CONSUMER FINANCIAL PROTECTION BUREAU (CFPB)

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

FANNIE MAE

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC)

FEDERAL RESERVE BOARD (FRB)

FEDERAL TRADE COMMISSION (FTC)

FREDDIE MAC

LEGINFO - 50 STATES

NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

The information contained herein is general in nature and not a substitute for internal policy. Readers are advised to confer with applicable supervisory agencies, legal or technology advisors. Contents of this material is based upon information available as of November 2025.

Information Security Requirements

CONTENTS

6 Fannie Mae Requirements

7 Freddie Mac Requirements

SECTION 1

Nonbank Model Data Security Law

Conference of State Bank Supervisors

The Conference of State Bank Supervisors (CSBS) and state regulators work together to create consistent regulatory standards for nonbank firms through the adoption of model laws. CSBS' model laws provide a clear nationwide framework for state legislatures to enact, and state regulatory agencies to implement. Model laws provide businesses with consistent requirements and promote common standards and practices across the state system. The content provided in this chapter has been adapted from various CSBS resources.

The **Nonbank Model Data Security Law** is model statutory language that establishes comprehensive standards for data security in financial institutions. It provides a robust framework to protect sensitive information and mitigate cyber threats across the industry. The model law is largely based on the FTC Safeguards Rule, including the amendments effective from June 2023 and amendments announced in October 2023. By leveraging the existing applicability of the Safeguards Rule to state covered nonbanks, adopting the model law imposes minimal additional compliance burden. This alignment ensures a streamlined approach to data security regulations and facilitates smoother implementation for financial institutions.

The model law establishes ten elements that are required by nonbank financial institutions to include in their information security program. The ten elements include:

NONBANK MODEL DATA SECURITY LAW INFORMATION SECURITY PROGRAM REQUIREMENTS	
1	Designate a Qualified Individual to implement and supervise the company's information security program.
2	Conduct a risk assessment.
3	Design and implement safeguards to control the risks identified through the risk assessment. Regularly monitor and test the effectiveness of safeguards.
4	Train staff.
5	Monitor service providers.
6	Keep the information security program current.
7	Create a written incident response plan.
8	Require the Qualified Individual to report to the Board of Directors.
9	Notify the company's state Commissioner regarding Notification Events.
10	Create a written business continuity and disaster recovery plan.

By adopting the Nonbank Model Data Security Law, state regulators require financial institutions to meet and exceed data security standards, promoting a secure environment for customer information and reinforcing trust in the industry. As of November, 2025, the following states have adopted the model law:

- Connecticut
- Georgia
- Kansas
- Maryland
- Massachusetts
- Minnesota
- Nebraska
- Nevada
- New York
- North Dakota
- Rhode Island
- Washington

CSBS Model Data Security Law Guidance

State financial regulators are increasingly concerned with information security threats to U.S. financial systems. Cybercriminals can cause significant financial losses for institutions and consumers whose information may be revealed and/or stolen for illicit purposes. This guidance is intended as a basis for establishing a minimum set of information security safeguards and sets forth the supervisory expectation that addresses the company's risk profile. It is imperative that senior management take this issue seriously and be responsible for the organization's safeguards program.

This guidance applies to the handling of customer information and applies to all customer information in the company's possession, regardless of whether such information pertains to individuals with whom the company has a relationship, or pertains to the customers of other institutions that have provided information. In general, the terms used in this guidance have the same meaning as set forth in the Federal Trade Commission's Safeguards Rule, which can be found at: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314.

Standards for Safeguarding Customer Information

The model law requires companies to develop, implement, and maintain a comprehensive, written Information Security Program that contains administrative, technical, and physical safeguards that are appropriate to the company's size and complexity, the nature and scope of activities, and the sensitivity of any Customer Information at issue. The Information Security Program should be designed to achieve the following objectives:

1) Ensure the security and confidentiality of Customer Information;
2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4) Establish a written incident response plan and address business continuity and disaster recovery.

Elements of an Effective Information Security Program

Qualified Individual

The company should designate a qualified individual responsible for overseeing and enforcing the Information Security Program. This Qualified Individual may be employed by the company, be an affiliate, or a contracted service provider. The company should require the qualified individual to report in writing, at least annually, to the board of directors or senior management, the overall status of the information security program and compliance with this Guidance and any applicable information security laws or rules.

Information Security Oversight and Training

The company should Implement policies and procedures to ensure that personnel are able to enact your Information Security Program by providing personnel with security awareness training that is updated to reflect risks identified by the risk assessment.

Risk Assessment

Companies should base the Information Security Program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Companies should periodically reassess risks and the sufficiency of any safeguards in place or that are needed to address these risks.

Safeguards

To control the risks identified, the company should design and implement the appropriate safeguards including (this list is not exhaustive):

- *Access Controls* to authenticate and permit access only to authorized individuals and restrict access at physical locations containing Customer Information.
- *Encryption* of all Customer Information held or transmitted by the company.
- *Multi-factor Authentication* should be implemented for any individual accessing Customer Information, unless the company's qualified individual has approved the use of reasonably equivalent or more secure controls.
- *Secure Disposal of Customer Information:* Companies are required to develop, implement, and maintain procedures for the secure disposal of Customer Information in any format that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Third Party Service Providers

If the company uses the services of a third party, it should take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue and periodically assess their risk and the continued adequacy of their safeguards.

Incident Response Plan

The company should establish a written incident response plan designed to promptly respond to, and recover from, any Security Event materially affecting the confidentiality, integrity, or availability of customer information in your possession. Such incident response plan should address the following six areas:

1) Internal processes for responding to a security event;
2) Identification of clear roles, responsibilities and levels of decision-making authority;
3) External and internal communications and information sharing;
4) Identification of requirements for the remediation of any identified weaknesses in the company's systems and associated controls;
5) Documentation and reporting regarding security events and related incident response activities; and
6) The evaluation and revision of the incident response plan following a security event.

Recommendations for Larger Entities

The following recommendations are intended for larger, more complex entities, or entities relying heavily on technology, whose security profiles dictate more sophisticated or robust controls:

- *Audit Trails.* Include audit trails within the information security program designed to detect and respond to security events.
- *Practices for In-House Developed Applications.* Adopt secure development practices for in-house developed applications utilized by the company for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information.
- *Change Management.* Adopt procedures for change management to document, track, test, approve and perform system and environmental changes.
- *Policies for Authorized Users.* Implement policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

- *Penetration Testing and Vulnerability Assessments.* Regularly test or otherwise monitor the effectiveness of the company's safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into your systems. Monitoring and testing should include continuous monitoring or periodic penetration testing and vulnerability assessments where feasible. If continuous monitoring is not feasible, institutions should conduct annual penetration testing and/or biannual vulnerability assessments.

Notification Events

A notification event is the acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Companies should notify the [Commissioner/Appropriate Contact] as promptly as possible following a security event, by contacting [Contact Information].

Two tables are provided on the following pages which summarize the applicability, notification event, and notification obligations for banks and nonbanks. Content is adapted from CSBS resources.

SECTION 2

State Requirements

State regulators have increased enforcement actions against mortgage brokers and nonbank lenders that fail to comply with the Gramm–Leach–Bliley Act (GLBA) and the Federal Trade Commission (FTC) Safeguards Rule. The FTC's updated Safeguards Rule requires mortgage brokers, to implement written information security programs to protect borrower data.

All U.S. states require both depository and nondepository financial institutions to have an information security plan. While GLBA applies nationwide, most states have duplicated or expanded upon the federal laws for licensees regulated by their Department of Financial Institutions (DFI), Department of Banking, or similar agency.

States with explicit requirements as a condition of licensing or ongoing compliance	States requiring reference to GLB and FTC Safeguards Rule in NMLS licensing system
California	Florida
Connecticut	Georgia
Illinois	North Carolina
Maryland	Ohio
Massachusetts	Washington
Nevada	
New York	
Texas	
Vermont	

Status as of November 2025

Failure to maintain a plan can result in enforcement actions or license suspension. Companies have been fined for lacking written information security plans, encryption policies, or incident response procedures. Penalties vary by state but typically include civil fines between $25,000 and $250,000 per violation.

Enforcement actions can include cease-and-desist, consent orders requiring immediate corrective actions, required adoption and submission of a compliant information security plan, and mandated third-party audits for 12-24 months. A key violation is the absence of an incident response plan or breach notification procedure.

Common violations include the lack of a designated information security officer or program manager, employee training, weak encryption of sensitive data, and failure to oversee third-party vendors with access to customer data.

A 50-state summary which delineates regulatory statutes, typical penalties, and common remedies is provided on the following pages.

State	Regulator	Breach Statute	Typical Penalties	Common Remedies
Alabama	Alabama State Banking Department (ASBD)	Ala. Code §8-38-1 et seq. (DBPA)	Civil penalties under DBPA/UDAP; consent orders via licensing statutes	WISP, MFA, encryption, vendor oversight, incident response plan
Alaska	Division of Banking & Securities	Alaska Stat. §45.48.010 et seq.	Civil penalties; license conditions for unsafe practices	IR playbook, encryption, training, third-party risk mgmt.
Arizona	AZ Dept. of Insurance & Financial Institutions (DIFI)	A.R.S. §18-551 et seq.	Civil penalties; consent orders; license conditions	MFA, encryption, logging/monitoring, vendor controls
Arkansas	Arkansas Securities Dept. (Non-Depository)	Ark. Code §4-110-101 et seq.	Civil penalties; UDAP exposure; exams may impose conditions	WISP uplift, training, vendor diligence
California	Dept. of Financial Protection & Innovation (DFPI)	Cal. Civ. Code §1798.82; CCPA/CPRA	DFPI penalties case-dependent; CCPA: $2,500/$7,500 per violation	Independent assessments, encryption, MFA, vendor risk mgmt.
Colorado	Division of Real Estate / Attorney General (privacy)	Colo. Rev. Stat. §6-1-716	Civil penalties via CCPA (CO) & licensing; consent orders	IR timelines, encryption, deletion policies, vendor controls
Connecticut	Dept. of Banking	Conn. Gen. Stat. §36a-701b	Civil penalties; license conditions; consent orders	WISP, encryption, vendor agreements, audits
Delaware	Office of the State Bank Commissioner	6 Del. C. §12B-101 et seq.	Civil penalties via data breach law/UDAP; licensing actions	MFA, encryption, IR playbooks, staff training
Florida	Office of Financial Regulation (OFR)	Fla. Stat. §501.171	Civil penalties; UDAP; consent orders	Access controls, encryption, IR, third-party risk
Georgia	Dept. of Banking & Finance	O.C.G.A. §10-1-912 et seq.	Civil penalties; license conditions	WISP, MFA, vendor mgmt, monitoring
Hawaii	Division of Financial Institutions (DFI)	Haw. Rev. Stat. §487N-1 et seq.	Civil penalties; consent orders	Encryption, training, IR testing
Idaho	Dept. of Finance	Idaho Code §28-51-104/105 et seq.	Civil penalties; license conditions	Security program, MFA, vendor due diligence

SECTION 3

FTC Safeguards Rule

The Federal Trade Commission's Safeguards Rule took effect in 2003 and was amended in 2021 to keep pace with current technology. The Rule was created to protect the security of customer information. The FTC further amended the Rule in 2023 to require covered entities to report certain data breaches and security incidents. Those breach notification requirements took effect in May 2024. Contents provided in this section is adapted from the booklet published by the Federal Trade Commission entitled, *The FTC Safeguards Rule—What Your Business Needs to Know*.

The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that are not subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act (GLBA). An entity is a "financial institution" if it's engaged in an activity that is financial in nature or is incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956. The Rule lists examples of the kinds of entities that are considered financial institutions:

COVERED ENTITIES	
Mortgage Brokers	Wire Transfer Companies
Mortgage Lenders	Collection Agencies
Payday Lenders	Credit Counselors
Finance Companies	Financial Advisors
Account Servicers	Tax Preparation Firms
Check Cashers	Non-Federally Insured Credit Unions

In addition to the above, a new category called "finders" was added in 2021. Finders are companies that bring together buyers and sellers, and further negotiations and transaction consummation are completed within those two parties. The Rule contains additional information regarding financial institutions and exemptions from certain provisions. Even if a company was not covered by the original Rule, most business operations have undergone substantial transformation in the past two decades.

Information Security Program

The following elements must be included in an organization's information security program:

1) **Designate a Qualified Individual to implement and supervise the information security program.**

   The Qualified Individual can be an employee of the company or can work for an affiliate or service provider. The individual's qualifications must include familiarity with the company's business operations as well as an understanding of the cybersecurity requirements. If the individual works for an affiliate or service provider, that entity must also maintain an information security program that protects the business.

2) Conduct a risk assessment.

To formulate an effective information security program, an inventory must be completed to determine foreseeable risks and threats to the security confidentiality and integrity of customer information— both internal and internal. Companies need to identify what information they have and where it is stored. The risk assessment must be written and include criteria for evaluating those risks and threats.

3) Design and implement safeguards to control the risks identified in the risk assessment.

The Rule requires companies to implement and periodically review access controls. Risks must be considered for every instance where a person or entity has access to customer information. The company must consider whether there is a legitimate business need for such entities to have access to such information.

4) Know what you have and where you have it.

A fundamental step to effective security is understanding the company's information ecosystem. Managers must conduct a periodic inventory of data noting where it's collected stored or transmitted. Keep an accurate list of all systems devices platforms and personnel. Design your safeguards to respond with resilience.

5) Encrypt customer information on your system and when it's in transit.

If it's not feasible to use encryption, information can be secured by using effective alternative controls. Such controls must be approved by the Qualified Individual who supervises the information security program.

6) Assess your apps.

If the company develops its own apps to store access or transmit customer information—or if third-party apps are provided for those purposes— organizations must implement procedures for evaluating their security.

7) Implement multi-factor authentication for anyone accessing customer information.

For multi-factor authentication the Rule requires at least two of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token) and an inherence factor (for example, biometric characteristics). The only exception would be if the Qualified Individual has approved in writing the use of another equivalent form of secure access controls.

8) Dispose of customer information securely.

Customer information must be disposed using a secure method no later than two years after the most recent use of the information. The only exceptions are a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible.

SECTION 4

Gramm-Leach-Bliley Act (GLBA)

Privacy of Consumer Financial Information (Regulation P)

Regulated institutions must comply with Regulation P, implemented by the CFPB covering consumer privacy provisions of the Gramm-Leach-Bliley Act (GLBA). Companies must require all employees, affiliates, and service providers to provide notice to customers regarding the company's privacy policies and practices.

The notice must describe the conditions under which the company may disclose nonpublic personal information about consumers to nonaffiliated third parties. Lastly, the company must give consumers a method to prevent the disclosure of information to nonaffiliated third parties by "opting out" of that disclosure. Companies are required to comply with Regulation P for information sharing with any of the following:

- Credit Agencies
- Appraisers
- Designated Underwriters
- Mortgage Insurance Companies
- Mortgage Investors
- Document Preparation Companies
- Closing Agents
- Electronic Business to Business Portals
- Outsourced Quality Control Firms

Initial Privacy Notice Requirement

The company must provide a clear and conspicuous notice that accurately reflects the company's privacy policies and practices to both customers and consumers. A consumer is an individual who obtains or has obtained a financial product or service from the company. The notice must be given to a consumer before the company discloses any nonpublic personal information to a nonaffiliated third party if the disclosure is not authorized.

A customer is a consumer who has a continuing relationship with the company. Notice must be given no later than when the company establishes a customer relationship. If the company subsequently transfers the servicing rights to another financial institution, the customer relationship transfers with the servicing rights. The company is not required to provide an initial notice to a consumer if the company does not disclose any nonpublic personal information about the consumer to any nonaffiliated third party. Notice is also not needed where the company does not have a customer relationship with the consumer.

Annual Privacy Notice to Customers

The company must provide a clear and conspicuous notice to customers which accurately reflects the company's privacy policies and practices annually during the continuation of the customer relationship. "Annually" means at least once in any period of 12 consecutive months during which the customer relationship exists. The company may define the 12-consecutive-month period, but The company must apply it to the customer on a consistent basis. An institution is not required to provide an annual notice to a former customer.

Information to be Included in Privacy Notices

The company must provide the appropriate initial, annual and revised privacy notices and include the following items of information:

- The categories of nonpublic personal information that the company collects;
- The categories of nonpublic personal information that the company discloses;
- The categories of affiliates and nonaffiliated third parties to whom the company discloses nonpublic personal information; and
- The categories of nonpublic personal information about the company's former customers that the company discloses and the categories of affiliates and nonaffiliated third parties to whom the company discloses nonpublic personal information about its former customers.

If the company discloses nonpublic personal information to a nonaffiliated third party and no other regulatory exceptions apply to that disclosure, a separate statement of the categories of information the company discloses and the categories of third parties with whom the company has contracted must be provided. Disclosures must include an explanation of the consumer's rights to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties.

If the company discloses nonpublic personal information to third parties as authorized under the regulation, the company is not required to list those exceptions in the initial or annual privacy notices. When describing the categories with respect to those parties, it is sufficient to state that the company makes disclosures to other nonaffiliated companies.

SECTION 5

Interagency Guidelines

Federal Reserve Board Small Entity Compliance Guide

The FRB's Small Entity Compliance Guide is intended to help financial institutions comply with the **Interagency Guidelines Establishing Information Security Standards** (Security Guidelines). Content in this chapter has been adapted from the Federal Reserve Board of Governors' resources.

The Small Entity guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. Although the guide was designed to help financial institutions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, this guide only addresses obligations of financial institutions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting customer records and information.

Background and Overview of Security Guidelines

The Security Guidelines implement section 501(b) of the Gramm-Leach-Bliley Act (GLB Act) and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The Security Guidelines establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information.

The guidelines apply to financial institutions as defined under the GLBA, including:

- Banks
- Credit unions
- Savings and loans institutions
- Non-bank financial companies engaged in activities such as lending, investing, or providing financial advisory services.

Each of the requirements in the Security Guidelines regarding the proper disposal of customer information also apply to personal information a financial institution obtains about individuals regardless of whether they are the institution's customers ("consumer information"). Consumer information includes, for example, a credit report about:

- An individual who applies for, but does not obtain a loan;
- An individual who guarantees a loan;
- An employee; or
- A prospective employee.

A financial institution must require, by contract, its service providers that have access to consumer information to develop appropriate measures for the proper disposal of the information.

Under the Security Guidelines, each financial institution must:

- Develop and maintain an effective information security program tailored to the complexity of its operations, and
- Require, by contract, service providers that have access to its customer information to take appropriate steps to protect the security and confidentiality of this information.

The standards set forth in the Security Guidelines are consistent with the principles the Agencies follow when examining the security programs of financial institutions. Each financial institution must identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary. If an Agency finds that a financial institution's performance is deficient under the Security Guidelines, the Agency may take action, such as requiring that the institution file a compliance plan.

Distinction between the Security Guidelines and the Privacy Rule

The requirements of the Security Guidelines and the interagency regulations regarding financial privacy (Privacy Rule) both relate to the confidentiality of customer information. However, they differ in the following key respects:

- The Security Guidelines address **safeguarding** the confidentiality and security of customer information and ensuring the proper disposal of customer information. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access or use of, that information. The Security Guidelines provide that financial institutions must contractually require their affiliated and non-affiliated third party service providers that have access to the financial institution's customer information to protect that information.

- The Privacy Rule limits a financial institution's **disclosure** of nonpublic personal information to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's nonpublic personal information to a nonaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure. The Privacy Rule requires that privacy notices provided to customers and consumers describe the financial institution's policies and practices to protect the confidentiality and security of that information. It does not impose any other obligations with respect to safeguarding customers' or consumers' information.

SECTION 6

Fannie Mae

Information Security and Business Resiliency Requirements

Effective 8/12/2025

Fannie Mae requires all approved lenders, servicers, and third-party originators (TPOs) to maintain robust information security and data protection programs. These programs must safeguard borrower and loan data throughout the mortgage lifecycle and apply to direct lenders, correspondents, brokers, subservicers, and integrated technology providers. Fannie Mae's expectations align with multiple federal and industry frameworks, including the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, CFPB Service Provider Guidance, and FFIEC Cybersecurity Guidelines.

Lenders must maintain a Written Information Security Program (WISP) that is approved by senior management and managed by a designated Information Security Officer (ISO). The program must include governance processes, risk assessments, control monitoring, and documented cybersecurity policies.

Fannie Mae Information Security and Business Resiliency Supplement

This section includes reference points, summaries, and certain abbreviated content from Fannie Mae's Information Security and Business Resiliency Supplement (the Supplement) dated September 2, 2025. Please refer to the Supplement to view the full scope of requirements for Seller/Services and their third-party vendors on the Fannie Mae website at:
https://www.fanniemae.com/media/54736/display

Information Security Program

Covered in Section 3 of the Supplement: the Company, or its affiliate (to the extent the affiliate's program covers the Company), at its own cost and expense, must:

- Implement an information security program with appropriate technical and organizational measures that, at a minimum, include the requirements of this Supplement (referred to as "Information Security Program");
- Align its Information Security Program with, or exceed, a current industry standard such as the National Institute of Standards in Technology (NIST) Framework or the International Organization for Standardization (ISO) 27001 Standard;
- Designate and keep a senior executive responsible for the development, implementation, and maintenance of its Information Security Program;
- At least annually, review its Information Security Program, including associated programs, plans, policies, standards, and procedures, to ensure alignment with this Supplement and current industry best practices;

- Communicate the requirements of its Information Security Program to all applicable Company employees, contractors and other personnel;
- Make its Information Security Program, with supporting documentation, available to Fannie Mae upon Fannie Mae's request; and
- Annually provide a written attestation executed by a duly authorized corporate officer that the Information Security Program and its associated programs, plans, policies, standards, and procedures meet the requirements of this Supplement. For SF Lenders, this attestation may be provided through the annual Form 582 process described in the SF Guides.

The Company must exercise at least the same level of care with Fannie Mae systems and Fannie Mae Confidential Information as it does for its own systems and Confidential Information.

The Company's Information Security Program must include programs, plans, policies, standards and procedures related to the topics listed below. The chart below indicates the section number of the Supplement for each topic required in the program.

FANNIE MAE Information Security Program Requirements	
Supplement Section #	Topic
3.1	Access Management
3.2	Human Resource Security
3.3	Audit and Accountability
3.4	Vulnerability
3.5	Physical and Environmental Controls
3.6	Cyber Incident Management and Response
3.7	Asset Management
3.8	System Development and Change Management
3.9	Patch Management
3.10	Data Protection and System Security
3.11	Mobile Computing
3.12	Network Security and Management
3.13	Cloud Computing
3.14	Supply Chain Risk Management

SECTION 7

Freddie Mac

Overview of information security and business continuity planning requirements

Guide Section 1302.1
Effective 09/11/2025

(a) Information security, business continuity and disaster recovery planning

This chapter contains the minimum information security program requirements Seller/Servicers must implement to reduce the impact and likelihood of unauthorized persons (or authorized persons with malicious or unlawful intentions) from gaining access to Freddie Mac's proprietary information, data and Protected Information in:

- Systems, as defined in Section 2401.1(b)
- Seller/Servicers' files, records, storage facilities and systems
- Files, records, storage facilities and systems of any Related Third Party

This chapter also includes the minimum requirements for a Seller/Servicer's business continuity plan and disaster recovery plan to support continuation of critical business processes necessary to comply with the Seller/Servicer's Purchase Documents.

(b) Minimizing Freddie Mac's risk of loss

To minimize Freddie Mac's risk of loss in the event of a disaster or unexpected disruption to critical business processes, a Seller/Servicer must have and maintain an information security program, business continuity and disaster recovery plan(s) that ensure its ongoing ability to conduct business operations with Freddie Mac. Information security program, business continuity plan and disaster recovery plan requirements must extend to the confidentiality, integrity and availability of Freddie Mac confidential information (as defined in Section 1201.8(a)) and Protected Information (as defined in Section 8101.4(d)) retained by a Seller/Servicer following Freddie Mac's termination of the Seller/Servicer's right to sell or service Mortgages.

(c) Information security, business continuity and disaster recovery

The information security, business continuity and disaster recovery minimum requirements (together, the "Minimum Requirements") are not intended to replace the Seller/Servicer's standards, policies and procedures but are intended to require certain minimum controls that must be in place as part of such standards, policies and procedures.

If a Seller/Servicer's regulator has established information security and/or business continuity plan and/or disaster recovery plan requirements that exceed Freddie Mac's Minimum Requirements, or if a provision of the Guide or the Seller/Servicer's other Purchase Documents requires more stringent minimum requirements, then the more rigorous requirements shall apply.

A Seller/Servicer's compliance with the Minimum Requirements will not relieve the Seller/Servicer from any liability arising or accruing under any other provision in the Purchase Documents. A Seller/Servicer's failure to comply with the Minimum Requirements may result in termination of the Seller/Servicer's access to any or all Systems. In addition, Freddie Mac may take other actions available under the Guide, the Seller/Servicer's other Purchase Documents, any user agreement or law.

The National Institute of Standards and Technology and International Organization for Standardization/International Electrotechnical Commission provide detailed guidance on the components of a successful information security program, business continuity plan and related activities. Seller/Servicers are strongly encouraged to review these standards and guidance to ensure their practices align with industry best practices.

Information Security

Guide Section 1302.2
Effective 9/11/2025

(a) Defined terms

Seller/Servicers should be familiar with the following defined terms as they relate to information security requirements:

- Authentication: the process in which a system verifies the identity and role of an individual, usually based on some form of credential(s) (password/ID, token, etc.).
- Encryption: the process of encoding or obfuscating messages or information in such a way that only authorized parties can read it.
- Vulnerability Management: the process of identifying and testing known software vulnerabilities within a system and prioritizing remediation according to each vulnerability's likelihood of occurrence and how the exploitation of the vulnerability would impact the system.

b) Information Security Minimum Requirements

(i) Information security program

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.