Fannie Mae

Fannie Mae Information Security and Business Resiliency Supplement

1. Introduction

The Fannie Mae Information Security and Business Resiliency Supplement (the "**Supplement**") contains information security, incident management, and business resiliency requirements with which a Company (defined below) must comply. All obligations required to be performed by the Company under this Supplement may be performed by a Company affiliate on the Company's behalf.

2. Relevant Terms

For the purposes of this Supplement, the following terms have the meaning given below:

Definitions	
Term	**Definition**
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Back-up	A copy of files and programs made to facilitate recovery, if necessary.
Business Continuity Plan	Plan that is developed and maintained to sustain enterprise operations, resiliency capabilities, contingency planning, and other processes during a disruption (e.g., disasters, technology disruptions).
Business Continuity Procedures	Procedures to continue operations if adverse conditions occur, such as a storm; a fire; a crime; a disruption of critical servicing functions; or the termination or expiration of a contract that is material to Company's ability to originate loans for sale to Fannie Mae, service Fannie Mae loans, comply with the Lender Contract or abide with other obligations and agreements the Company has or relates to business conducted with Fannie Mae.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Company	With respect to this Supplement, a "Company" means a Single Family ("**SF**") Lender, or Multifamily ("**MF**") Lender.
Confidential Information	Any information, whether written, oral, visual, or electronic, that is disclosed by one party to another, directly, or indirectly, which is designated as confidential, proprietary, or trade secret information or that a reasonable person would recognize to be confidential given the nature of information and the circumstances of the disclosure. This includes:

Definitions	
Term	**Definition**
	(a) information that is not a matter of public knowledge or which is specifically designated as confidential, including nonpublic personal information, business plans, trade secrets, product development strategy and activity, product concepts and features, marketing strategy, corporate assessments and strategic plans, pricing, financial and statistical information, accounting information, meta data, identity of suppliers or clients, customer lists, software (including source code and object code), technical specifications, systems, processes, formulae, inventions, discoveries, developments, designs, drawings, models, algorithms, flow charts, technology previews, and other documentation policies, guidelines, procedures, practices, disputes, or litigation; and (b) compilation or summary information or data that contains or is based on the foregoing. Confidential Information includes Fannie Mae Confidential Information.
Consolidated Technology Guide	The Fannie Mae Consolidated Technology Guide, as amended, restated, supplemented, or otherwise modified from time to time.
Cybersecurity or Data Breach Incident (collectively "Cybersecurity Incident")	Any of the following related to Confidential Information: • loss of; • accidental or unauthorized acquisition, use, modification, disclosure, deletion, or destruction of; • accidental or unauthorized access to; • circumvention, disabling, or deactivation of security measures protecting; or • occurrence affecting the confidentiality, integrity, or availability of Examples include one or more of the following occurring at the Company or at the Company's third party(ies): • ransomware; • denial of service attack which may affect the delivery of the services to Fannie Mae; • business e-mail compromise (BEC); and • Vulnerabilities that may affect the delivery of services or loans to or for Fannie Mae.

Definitions	
Term	**Definition**
Disaster Recovery Procedures	Procedures to recover and protect Company business information, technology and infrastructure in the event of a disaster.
Encryption	The cryptographic transformation of data. Synonymous with encipherment. The result of Encryption is cipher-text. The reverse process is called decryption.
Fannie Mae Confidential Information	Means Confidential Information about Fannie Mae borrowers, collateral securing a Fannie Mae loan, Fannie Mae data, including all servicing data related to loans serviced for Fannie Mae, existing or proposed Fannie Mae technologies, products or services and Fannie Mae's business when performing underwriting, origination, selling, servicing or other activities under Company's contracts with Fannie Mae. Fannie Mae Confidential Information under this Supplement includes anything that would be defined as Confidential Information under the SF Guides for SF Lenders and under the MF Guide for MF Lenders.
Include, including and similar derivations	Means including, without limitation.
Lender Contract	For SF Lenders, has the meaning attributed to such term in the SF Guides and for MF Lenders, has the meaning attributed to such term in the MF Guide.
MF Guide	Collectively, the Multifamily Selling and Servicing Guide, Multifamily Program Rules, and the Consolidated Technology Guide
MF Lender	A "Lender" as defined in the MF Guide.
Multi Factor Authentication or MFA	Authentication using two or more factors to achieve authentication. Factors include: • something you know (e.g. password/personal identification number (PIN)); • something you have (e.g., cryptographic identification device, token); or • something you are (e.g., biometric)

Definitions	
Term	**Definition**
SF Selling Guide	The Selling Guide – Fannie Mae Single Family, as amended, restated, supplemented, or otherwise modified from time to time.
SF Servicing Guide	The Servicing Guide – Fannie Mae Single Family, as amended, restated, supplemented, or otherwise modified from time to time.
SF Guides	Collectively, the SF Selling Guide, SF Servicing Guide and Consolidated Technology Guide.
SF Lender	A "lender," as described in the SF Selling Guide. SF Lender includes sellers, servicers and seller/servicers as appropriate.
Vulnerability	Weakness in an information system, software, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

3. Information Security Program

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 following, as more particularly described in the subsections below:

- Access Management
- Human Resource Security
- Audit and Accountability
- Vulnerability Management
- Physical and Environmental Controls
- Cyber Incident Management and Response
- Asset Management
- System Development and Change Management
- Patch Management
- Data Protection and System Security
- Mobile Computing
- Network Security and Management
- Cloud Computing
- Supply Chain Risk Management

3.1 Access Management

Identification and Authentication are one of the first lines of defense in network security. These access management controls are the technical measures that prevent those, without reason, from entering a system and accessing Confidential Information. They are the controls that establish the identities interacting with a system.

Access Management Requirements	
✓	**At a minimum, the Company's access management program must include**
	A strategy and process for enforcing acceptable access to and use of information systems. Procedures must include: • steps for approving access;

Access Management Requirements	
	• removing access upon termination or transfer; • evaluating inactivity; and, • determining when access is otherwise no longer needed. Access for all human and non-human (system) user accounts should be reviewed and certified by the entitlement owner or user manager at least annually to ensure access is limited to only authorized users;
	Requirements and processes for managing privileged accounts, including monitoring changes to roles or attributes and enforcing an access revocation process, to ensure timely removal of dormant accounts and access that is no longer required for the assigned user such as when the user has terminated employment;
	Requirements for the use of Multi-Factor Authentication, where applicable;
	Remote access requirements, including mechanisms to monitor and control remote access;
	Requirements for locked accounts after multiple failed logins attempts and timeout requirements for inactivity;
	Least privilege access control methods that limit access to users on a need-to-know basis; and
	Guidelines and requirements for: • password complexity, • reuse timelines for passwords, • account lockout, • password change timelines, and • storage of passwords. Every user must have a unique user ID; no shared accounts may be used beyond built-in and system accounts where individual usage can be tracked.

The Company must also require employees and system accounts (non-human ids) to Authenticate to a system or application through a private and controlled method. Methods or Authentication processes include user passwords, personal identification numbers and token devices. MFA must be implemented for access to privileged accounts.

3.2 Human Resource Security

Users of a Company system play a role in protecting that system and no system can be secure without addressing personnel security. Appropriate levels of system access, informing users of their responsibilities, and training them on security requirements help a system's security posture.

✓	Human Resource Security Requirements
	The Company must have a formal on-boarding process that includes steps to complete background verifications for all employee candidates and contractors that will have access to Fannie Mae Confidential Information or Fannie Mae systems (either directly or through indirect means such as an application programming interface or an interface that allows for such integration to Fannie Mae systems).
	The Company must require employees, contractors and any other authorized parties working through the Company or on its behalf to comply with a code of conduct or other similar policies, standards and procedures that include an attestation of compliance prior to gaining access to Fannie Mae Confidential Information or Fannie Mae systems. The code of conduct or policies, standards and procedures must include, at a minimum, requirements for the following: • the protection of, confidentiality of, privacy considerations of, and non-disclosure requirements relating to Fannie Mae Confidential Information and Fannie Mae systems; • the appropriate use of Company's assets; • record management; and • conflicts of interests.
	At least annually, the Company must conduct an information security awareness training to all employees, contractors and other authorized parties working through the Company that have access to Fannie Mae Confidential Information or Fannie Mae systems. Training topics should include: • security awareness, including an overview of Company's Information Security Program and emerging risks/threats; • roles and responsibilities (expectations); and • reporting obligations and data retention.

3.3 Audit and Accountability

Audit and accountability are a risk management strategy and contribute to the Company's overall privacy and security posture.

Audit and Accountability Requirements	
✓	**The Company must:**
	Develop, implement, and maintain written requirements for the logging and monitoring of activities and actions within its information systems. Requirements should include log retention periods and expectations for handling logs to ensure logs retain relevant, useable, and timely information sufficient to identify user access and system activities;
	Implement controls to ensure logs are protected from access, modification, or deletion by unauthorized personnel;
	Establish processes and controls that ensure logs are monitored and reviewed for the unauthorized disclosure, modification, deletion, or replications of Confidential Information; and
	Perform an independent security assessment of the control environment upon the occurrence of any Cybersecurity Incident (except as otherwise mutually agreed to below) and at least annually. Such independent assessment must be done by a qualified independent auditor not affiliated with the Company. The Company must remediate findings relevant to the services provided to or on behalf of Fannie Mae or loans being sold to or serviced for Fannie Mae raised in any independent security assessment. Remediation must be completed within a commercially reasonable timeframe and consistent with standard industry practices. • Following a Cybersecurity Incident where access to Fannie Mae has been suspended pursuant to Section 4.1 below, an attestation may be substituted in place of an Independent Security Assessment if mutually agreed upon by both parties.

3.4 Vulnerability Management

Vulnerability management is an important part of an information security program and can help identify weaknesses in the Company's applications, systems, and network before those weaknesses are exploited.

Vulnerability Management Requirements	
✓	**The Company must have a documented vulnerability management program that includes:**
	A process to identify, analyze and remediate identified Vulnerabilities within commercially reasonable timelines, including an inventory of all identified Vulnerabilities, a risk rating of their level of risk, and their remediation status based on a risk-based schedule;
	An independent third-party penetration test that is conducted at least annually on systems or system components used to store, access, process or transmit Confidential Information or connect to a Fannie Mae system; and
	Vulnerability scanning/testing conducted on a regular basis.

3.5 Physical and Environmental Controls

Physical and environmental controls help protect the physical components of the Company against threats associated with its environment.

✓	Physical and Environmental Control Requirements
	The Company must implement a physical security control program that governs the Company's buildings and facilities (owned or leased), including those that contain information systems.
	The program must establish controls designed to detect, monitor, and prevent unauthorized access and to respond to physical security incidents.
	The program must include: • An ongoing and updated inventory of individuals gaining access to buildings and facilities containing information systems with periodic review of such access at least annually; • Measures to ensure only authorized access to buildings and facilities that contain information systems (e.g., badges, badge scanners, etc.) and monitor for intrusions through cameras, guards, or other means to help protect the Company's infrastructure; • Steps to remove physical and logical access immediately upon the voluntary or involuntary departure of an authorized individual and/or an individual no longer needing access to a physical space;

✓	Physical and Environmental Control Requirements
	• Steps and controls to limit access to sensitive and restricted areas (media, network rooms, vaults, etc.) to only authorized individuals on a need-to-know basis following least privileged access protocols; and • Environmental controls to prevent and mitigate the disruption to operations and data integrity caused by natural disasters or human-caused incidents.

3.6 Cyber Incident Management and Response

The financial services sector is frequently targeted by cyber attacks. Having a Cybersecurity Incident management and response framework can help mitigate the harmful effects of a Cybersecurity Incident. A properly managed program can help with detecting a Cybersecurity Incident, understanding potential losses following a Cybersecurity Incident, and support the restoration of the Company resources.

Cyber Incident Management and Response Requirements	
✓	The Company must
	Maintain an up-to-date incident response plan that includes incident response policies, standards and procedures that: o identify required resources for the plan, including the management support needed to effectuate the incident response plan; o identify roles and responsibilities for incident response stakeholders; o provide mobilization contact and call trees; o offer severity assessment requirements; o log recording steps and processes for evidence collection; o provide steps for executing incident response capabilities.
	Complete, on at least an annual basis, a test of the incident response plan and capabilities and incorporate lessons learned from tests into the incident response plan; and
	Provide notification to Fannie Mae of any disruptions, including those related to technology, which may impact operations that could potentially impair, or impact business conducted with Fannie Mae or the Company's ability to perform its obligations under its contracts with Fannie Mae. Disruptions rising to the level of a Cybersecurity Incident must be reported in accordance with requirements noted in Section 4 of this Supplement.

3.7 Asset Management

In this Supplement, asset management is an umbrella term referring to the controls for:

- system configuration;
- system maintenance; and
- system and services acquisition.

Managing Company configurations helps prevent one system change from adversely impacting another system. System maintenance can help with the continued security, reliability, and performance of the Company's systems which includes information security practices such as patch management, configuration management, and access management. System and services acquisition provides the Company an opportunity to understand its third party(ies) Information Security practices and maintain appropriate oversight and controls of their activity.

Asset Management Requirements	
✓	As part of the Company's access management program, the Company must:
	Create and execute a process for developing and maintaining secure configuration baselines for infrastructure components;
	Implement mechanisms to detect and manage the installation of unapproved software;
	Maintain an inventory management system to track physical and software assets, such as end-user technology, servers, network devices, applications, and their corresponding asset ownership. The Company must reconcile the inventory management system periodically to verify all assets are included;
	Implement documented procedures detailing guidelines and requirements for tracking the removal of technology assets; and
	Conduct periodic maintenance on systems and technology to ensure protections and systems remain up to date with latest supported versions and settings.

3.8 System Development and Change Management

If the Company develops, deploys, updates, or maintains applications or tools that will access, store, or process Confidential Information or that will connect to a Fannie Mae system, the Company must implement and maintain a formal Software Development Life Cycle ("**SDLC**") policy, standard or supporting procedures.

System Development and Change Management Requirements	
✓	**The SDLC policy, standard or procedures must include:**
	Requirements for secure coding;
	Code development and scanning pre-and post-deployment;
	Separation between development/testing and production environments;
	Testing to validate functional and non-functional requirements are met prior to production;
	Requirements for managing, remediating, and reporting on defects;
	Requirements for documenting and assuring currency of software bill of materials; and
	Requirements on assessing Vulnerabilities in using third party code (including open-source code).

All changes to the Company's technology environment (including new hardware, upgrade to systems, patches, etc.) must follow a formal change management process including tracking, testing, and documented back-out procedures that reverts to the previous state if a change is unsuccessful.

3.9 Patch Management

The Company must:

- implement and maintain a written patch management program, and associated policies, standards and procedures; and
- perform timely software updates and patches based on the Company's Vulnerability management program, and maintain a process for testing and ensuring software updates and patches are consistently applied as they become available without compromising the confidentiality, integrity, and availability of Fannie Mae Confidential Information.

3.10 Data Protection and System Security

System and communications protection controls help maintain the confidentiality and integrity of information at-rest and in-transit. System and information integrity controls help ensure data has not been altered or damaged.

✓	Data Protection and System Security Requirements
	The Company must implement technical security measures designed to detect, mitigate, and prevent malicious and unauthorized use of technology assets.
	The Company must: • Install anti-virus software to protect servers and end user systems or utilize endpoint detection and response tools with an anti-virus component; • Keep all software up to date with supported versions according to a Company software update policy, standard, or procedure; • Implement and maintain preventive controls and intrusion detection designed to identify potential threats and security compromises; and • Establish a threat management process with steps to manage security threats as they are identified.
	The Company must also implement controls to properly identify, classify and protect Confidential Information. These controls include: • Maintaining a formal data management and Encryption use policy, standards or procedure and prohibit use of outdated technologies which have identified Vulnerabilities or are no longer supported by the software developer; • Identifying and controlling access, use, security, and confidentiality of Fannie Mae Confidential Information. Access to sensitive information must be limited to only authorized users commensurate with their role and responsibilities on a need-to-know basis; • Encrypting end user devices (laptops, tablets, cell phones) to protect data if devices are lost or stolen; • Encrypting data in-transit and at-rest; • Maintaining a data loss prevention/transmission protection process including data loss prevention controls and corresponding management process to identify Confidential Information stored on media and outgoing transmissions over public communication; and • Restricting the transfer of data to USB, other removable media devices and non-Company systems unless expressly permitted and subject to the same protections outlined in this Supplement.

3.11 Mobile Computing

The Company must maintain mobile device/computing management policies, standards and procedures that, at a minimum, include requirements for:

- Approved and prohibited mobile applications and measures to ensure software updates are applied and kept current;

- Encryption mechanisms to ensure data security; and,
- Identity and access management requirements.

If Company uses digital media, non-digital media, or mobile media, it must provide protections to:

- restrict access and make the media available to authorized personnel only;
- apply appropriate security labels to system media ; and
- provide instructions on how to remove information from media such that the information cannot be retrieved or reconstructed.

3.12 Network Security and Management

✓	Network Security and Management Requirements
	The Company must: • Implement information technology controls such as firewalls to block all inbound traffic from, and outbound traffic to public networks unless permitted by policy, standards or procedures; • Manage and restrict ports, protocols, and services to only those that are required and approved for business operations; • Implement mechanisms to monitor network traffic and detect anomalous network traffic; • Review and approve firewall rules on a defined frequency and whenever a notable change in network technology occurs; and • Control, secure, and monitor wireless access points.
	In addition, if the Company offers wireless networks for network users, the Company must: • Implement and keep up to date a Wireless Local Area Network (WLAN) Authentication method that meets or exceeds the current industry best practices on Encryption strength and technology; • At least annually, perform reviews of approved wireless networks to validate and verify authorized users and access points; and • Implement controls, including password protection, to ensure access to routers and network devices are appropriately restricted to only authorized users and administrators.

3.13 Cloud Computing

Cloud Computing provides the Company access to pooled resources (including applications, storage, and networking) and can help optimize performance and provide

scalability. It is a cost-effective and flexible solution for data and application management. Cloud Computing controls can help the Company manage its relationship with cloud service providers and implement secure by design solutions.

✓	Cloud Computing Requirements
	If the Company leverages Cloud Computing to store, process, access, or transmit Confidential Information or connect to a Fannie Mae system, it must establish cloud computing policies, standards or procedures. The policy, standards or procedures must define the Company's cloud strategy and ensure there are adequate steps in place to use cloud service providers with adequate controls for Cloud Computing.
	The Company must also understand its security posture, concentration risk, and related dependencies when using Cloud Computing.
	The Company must: • use cloud providers that base their services on current technology, with regular upgrades to state-of-the-art technology which has been tested for security and functionality; • implement identity access management procedures consistent with this Supplement for accessing data and services in the cloud; • use cloud services that are available, responsive, and consistent; • secure access to the Company's cloud environment consistent with this Supplement; and • utilize secure-by-design principles.

3.14 Supply Chain Risk Management

Modern computing uses system interconnection and a distributed, global supply chain. The Company and Fannie Mae could be harmed if the cybersecurity risks associated with the Company's supply chain are not understood or addressed. Controls for supply chain risk provide an understanding of the supply chain based on the Company's unique business model and also provide an oversight mechanism for the Company's third parties.

✓	Supply Chain Risk Management Requirements
	The Company must develop, document, and implement a formal vendor risk management program to ensure the controls of new and existing vendors align with and are at least as protective as the Company's Information Security Program and those required in this Supplement.

✓	Supply Chain Risk Management Requirements
	The vendor risk management program must include policies, standards, and procedures to measure and assess risk and impacts to business operations from a Company's use of vendors.
	Vendor re-assessments for existing relationships should be conducted on a risk-based frequency.
	The Company must have an agreement in place with each vendor that covers adequate considerations for security and resiliency consistent and in compliance with the requirements noted in this Supplement. The Company is responsible for its vendors' compliance with the obligations in this Supplement and for all failures by a vendor to comply with this Supplement to the same extent as if such failure were committed by the Company.

4. Cybersecurity Incident Management

If the Company experiences a Cybersecurity Incident, or an information security professional could reasonably conclude the Company (or its third parties) may have experienced a Cybersecurity Incident:

✓	The Company must:
	Promptly investigate, correct, and mitigate the Cybersecurity Incident at the Company's expense, including identifying all Fannie Mae Confidential Information affected by the Cybersecurity Incident and taking measures designed to prevent the continuation and recurrence of the Cybersecurity Incident.
	Without undue delay and no later than 36 hours after identification of the Cybersecurity Incident, or the reasonable conclusion a Cybersecurity Incident may have occurred, and promptly thereafter as requested, provide Fannie Mae via e-mail at privacy_office@fanniemae.com (or by such other means as Fannie Mae may otherwise request) all known details of the Cybersecurity Incident, including: • related internal and external investigations and technical indicators of compromise (e-mail addresses, hash values, IP addresses, malware code, indicator of compromise, etc.); • all tactics, techniques, and procedures associated with the incident, details surrounding the attack methodology, timing of the incident, and whether Fannie Mae's systems or Fannie Mae Confidential Information have been accessed or otherwise compromised; • the name(s) of any third-party incident response or remediation service providers with whom Company is working; • any law enforcement agencies that the Company has engaged;

✓	The Company must:
	• contact information and titles for the individual(s) leading the Cybersecurity Incident investigation within or on behalf of the Company; and • details and information as to whether and if so, the extent to which Fannie Mae Confidential Information, was accessed, taken, or exposed.

Fannie Mae may request meetings with the Company to discuss the Cybersecurity Incident and may request additional documents and other assistance necessary to help Fannie Mae gather the information necessary to help protect Fannie Mae systems, loans and information and identify any potential impact to Fannie Mae resulting from the Cybersecurity Incident. To the extent not prohibited by law, the Company must cooperate with Fannie Mae for any requests for additional documents and other assistance regarding the Cybersecurity Incident.

4.1 Actions by Fannie Mae

Depending upon the nature of the Cybersecurity Incident, Fannie Mae, at its sole discretion, may, without prior notice to the Company, immediately take one or more of the following actions:

- Block e-mail access to Fannie Mae e-mail domains;
- Implement a forced password reset for Company users with access to Fannie Mae systems;
- Disable or terminate the Company user or system access to Fannie Mae systems, including suspending any integration interfaces and application programming interfaces between any Company-licensed or -owned software and Fannie Mae systems; and
- Terminate or suspend the Company's license to one or more Fannie Mae applications.

If disabled, the Company's access and integration to Fannie Mae systems will be restored only after the Company provides an attestation as to the security and safety of its systems and satisfies any other conditions Fannie Mae may impose. Such an attestation may be provided to Fannie Mae either by an independent third-party investigative service provider the Company has retained or be a signed statement by two officers of the Company attesting to the safety and security of its systems.

4.2 Filings by the Company

Notwithstanding the foregoing, if a Company has filed a Form 8-K, Form 6-K, or other Cybersecurity Incident disclosure with the Securities and Exchange Commission, or has made any other filings with a regulatory body, relating to a Cybersecurity Incident, the Company must provide a link to or copy of such filing to Fannie Mae via e-mail at privacy_office@fanniemae.com (or by such other verified means as Fannie Mae may otherwise request or may be required based on Cybersecurity Incident type) within 36

hours of the day on which the form was filed. This obligation is in addition to the general obligation to provide notification under this section.

4.3 Additional Company Requirements

While investigating a Cybersecurity Incident that impacts or could potentially impact Fannie Mae Confidential Information (e.g., lost/stolen file; misdirected mailing; Company or third-party Cybersecurity Incident; etc.), the Company must follow or be subjected to the steps outlined above, as applicable, and in addition follow the requirements below:

✓	The Company must:
	Inform the Fannie Mae Privacy Office via e-mail at privacy_office@fanniemae.com (or by such other verified means as Fannie Mae may otherwise request or may be required based on Cybersecurity Incident type) of the details regarding the incident, to include: the number of individuals impacted, from what jurisdictions, the company(ies) involved if there is more than one entity, description of the related nonpublic personal information ("**NPI**"), and root cause,;
	Provide timely written notice to affected borrowers, other impacted parties and any state or federal agencies or other governmental bodies in accordance with applicable privacy, data security and notification laws and regulations and maintain a copy of the notice in the individual loan file;
	Request permission from Fannie Mae's Privacy Office to use Fannie Mae's name if the Company intends to refer to Fannie Mae in any notices sent to affected borrowers or regulatory bodies; and
	Promptly following a request by Fannie Mae, provide Fannie Mae and its designees all information and assistance needed to enable Fannie Mae to evaluate the need for, and to timely make, any notification it deems necessary or advisable concerning the Cybersecurity Incident.

A Company notification to Fannie Mae or Fannie Mae's response to a Cybersecurity Incident under this section is not an acknowledgment by Fannie Mae of any fault or liability with respect to the Cybersecurity Incident. Notwithstanding anything required in this Cybersecurity Incident Management section, the Company is fully and solely responsible for fulfilling all third-party notification obligations related to any Cybersecurity Incident and complying with its obligations under applicable laws, rules and regulations including those related to privacy, data security, and incident notification.

4.4 Lost/Stolen/Incorrectly Routed Physical Information

If Company:

- Inadvertently or by intentional action, loses;

- Has stolen from; or,
- Incorrectly routes outside of Company;

physical information, such as paper files or other media, which includes Fannie Mae Confidential Information:

✓	**The Company must:**
	Promptly investigate, correct, and mitigate the matter at the Company's expense, including identifying all Fannie Mae Confidential Information affected by the matter and taking measures designed to prevent the continuation and recurrence of the matter.
	Without undue delay and no later than 36 hours after identification of the matter, or the reasonable conclusion one may have occurred, and promptly thereafter as requested, provide Fannie Mae via e-mail at privacy_office@fanniemae.com (or by such other means as Fannie Mae may otherwise request) all known details of the matter, including: • related internal and external investigations; • all tactics, techniques, and procedures associated with the matter, as applicable; • the name(s) of any third-party incident response or remediation service providers with whom Company is working; • any law enforcement agencies that the Company has engaged; • contact information and titles for the individual(s) leading the investigation within or on behalf of the Company; and • details and information as to whether and if so, the extent to which Fannie Mae Confidential Information, was accessed, taken, or exposed.

Fannie Mae may request meetings with the Company to discuss the matter and may request additional documents and other assistance necessary to help Fannie Mae gather the information necessary to help protect Confidential Information and identify any potential impact to Fannie Mae resulting from the matter. To the extent not prohibited by law, the Company must cooperate with Fannie Mae for any requests for additional documents and other assistance regarding the matter.

A Company notification to Fannie Mae or Fannie Mae's response to a reported matter under this section is not an acknowledgment by Fannie Mae of any fault or liability with respect to the reported information. Notwithstanding anything required in this section, the Company is fully and solely responsible for fulfilling all third-party notification obligations related to any reported matter and complying with its obligations under applicable laws, rules and regulations including those related to privacy, data security, and incident notification.

5. Business Continuity Management

Cybersecurity Incidents and other disruptions (such as natural disasters or termination of material contracts) have the potential to meaningfully impact the Company's business operations. Planning for these contingencies is a necessary step and a helpful mitigant to resulting impacts after a Cybersecurity Incident or other disruption (natural or human made disaster).

5.1 Business Continuity Plan

The Company must have a Business Continuity Plan that identifies business processes critical to the continuation of services and operations including those necessary to comply with obligations the Company has to Fannie Mae under the Lender Contract, other agreements the Company has with Fannie Mae, or that relates to business conducted with Fannie Mae.

The Company's Business Continuity Plan must:

- address Business Continuity Procedures and Disaster Recovery Procedures and provide a level of preparation, coordination, facilitation, resiliency, and testing that addresses disruptions that could impact normal operations and processing and
- ensure the Company's ability to recover critical business operations if:

  (A) there is a disruption or disaster, including to back-up systems, and

  (B) in the event of the expiration or termination of any contract that is material for the Company's sale or servicing of Fannie Mae loans or ability to comply with the Lender Contract or other agreements the Company has or relates to business conducted with Fannie Mae.

✓	**The Business Continuity Plan must meet or exceed industry standards and include requirements related to:**
	Threat assessment, business impact analysis and continuity plan;
	Identification of critical functions and resources required to sustain operations including documented workarounds, consideration of alternate processing facilities, disaster recovery systems and data back-ups;
	Moving business operations or recovering technology in another location if a disaster occurs at a worksite or data center;
	Alternate network and telecommunication capabilities;
	Recovery steps after a disruption;

✓	The Business Continuity Plan must meet or exceed industry standards and include requirements related to:
	Crisis management plan and communication strategy to clearly outline points of contact for both Fannie Mae and any vendor dependencies;
	Third party dependency information;
	Testing of the Business Continuity Plan annually at a minimum or when major changes occur to the Business Continuity Plan; and
	Governance to ensure compliance with Business Continuity Plan requirements.

The Business Continuity Plan must be available to all resources or staff that are required to support the execution of the plan.

5.2 Additional Requirements

✓	In addition, the Company must:
	Conduct an annual threat risk assessment to evaluate emerging resiliency risks and threats that could impact operations;
	Have a governing body in place to provide guidance and support of the Business Continuity Plan, ensuring the Business Continuity Plan is reviewed, formally socialized with leadership, and approved at least annually, or when material changes occur;
	Establish and document contingencies for third party and fourth party vendor and service provider relationships;
	Confirm the Company has the ability to recover critical business operations in the event that any third party vendors or service providers, such as subservicers, third-party originators, and outsourcing firms, used by the Company: • fail to maintain Business Continuity Procedures or Disaster Recovery Procedures, • suffer complete business failure or dissolution, or • experience the expiration or termination of any contract that is material for the Company's sale or servicing of Fannie Mae loans or ability to comply with the Lender Contract or other agreements the Company has or relates to business conducted with Fannie Mae;
	Perform related business continuity due diligence on its third parties to ensure they meet contracted service requirements and maintain a business continuity program that aligns with industry best practices;
	Establish business continuity planning strategies that includes loss scenarios for people, technology, data, facilities, and third parties;

✓	In addition, the Company must:
	Exercise its business and technology continuity planning documentation annually through tabletop or other similar exercises; and
	Document lessons learned and after actions when plans are tested or activated. Results should be shared with Company senior management and after actions should be tracked to resolution.

6. General Requirements

General Requirements	
Topic	**Description**
Amendments to this Supplement	Fannie Mae may at any time alter or waive any of the requirements of this Supplement, impose other additional requirements, or rescind or amend any provision in this Supplement. The Company must make sure its staff and third parties are thoroughly familiar with the content and requirements of this Supplement, as it now exists and as it may be changed from time to time. Fannie Mae will notify the Company of changes and updates to this Supplement via bulletin as described below.
Technical Issues	In the event of technical difficulties or system failures with Fannie Mae's website, or with delivery of bulletins, users may use the "Contact Us" link on the website to ask questions or obtain more information.
When Questions Arise	Questions about this Supplement can be e-mailed to your Fannie Mae point of contact.
Issued Bulletins; Amendments	Fannie Mae may issue hard-copy bulletins or electronic bulletins (via electronic mail or posted to an applicable Fannie Mae internet site) amending the Supplement on a prospective basis, effective on the date specified by Fannie Mae in the bulletin. Fannie Mae will issue each bulletin at least 20 calendar days before its effective date. The Company may reject any bulletin by providing written notice to Fannie Mae within 15 calendar days after receipt of such bulletin, in which case Fannie Mae may terminate the Company's Lender Contract effective as of the effective date of the bulletin or written notice. Unless the Company provides such rejection notice within the applicable period, the Company is deemed to have accepted such amendments, and

General Requirements	
Topic	**Description**
	such amendments will form part of this Supplement as of the effective date of such bulletin or written notice. The Company's continued sale to or servicing of loans for Fannie Mae is an acknowledgment of its acceptance. If a bulletin is not used, the terms of this Supplement may be amended by a writing executed by a duly authorized representative of each party to be bound thereby.
Conflicts	If there is any conflict between a term or condition in this Supplement and the Guide(s) to which the Company is subject, the term or condition contained in this Supplement will take precedence over the conflicting term or condition in the SF Guides (with respect to the SF Lenders) or MF Guide (with respect to MF Lenders) with respect to the subject matter stated in this Supplement.
No Implied Waiver	No term, provision, or clause of this Supplement will be deemed waived, and no breach excused unless such waiver or excuse is in writing and executed by a duly authorized representative of Fannie Mae. Any waiver by Fannie Mae of a breach by the Company does not constitute a consent to, waiver of, or excuse for any different or subsequent breach.
Construction	Headings and captions are for convenience only. If any provision of this Supplement is held invalid, the enforceability of all remaining provisions are not affected, and the Supplement will be interpreted as if the invalid provision were not contained in the Supplement.