October 10, 2018

eMortgage Systems Security Best Practices

The guidance below provides best practices to consider when developing your eMortgage systems and governing policies. Share this information with your IT and information security teams as they prepare to implement your eMortgage systems.

For more information on Freddie Mac eMortgage systems requirements, see the eMortgage Guide available on FreddieMac.com

Data Encryption

eClosing, eVault, eNote creation systems (systems) processing or storing sensitive data should prevent unauthorized viewing of sensitive data and documents through restricted access. Some recommended best practices for protecting the confidentiality and integrity of data in transit and at rest include, but are not limited to:

- Encryption algorithms compliant with National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) 140-2 guidance
- X.509 digital certificates for device/server-based TLS/SSL (Transport Layer Security/ Secure Sockets Layer) session authentication which support a minimum SHA-256 signing hash and TLS sessions that use a minimum of 2048-bit RSA key and 128-bit AES key

User Authentication

Systems processing or storing sensitive data should support multifactor authentication methods, such as combinations of unique user ID/password, S/Key, password tokens, biometrics, smart card authentication, and X.509 digital certificates.

Password policy governing user credentials should support:

- Storage of user passwords as a salted hash
- System lockout after 3 unsuccessful login attempts
- Required approval of accounts by authorized management prior to granting access
- Comply with NIST SP 800-63B guidance

Access Controls

Systems should support:

- Role-based access control
- Separation of duties through assigned authorizations
- Access protocols which adhere to principle of least privilege
- Limit the number of concurrent sessions for each account
- Detection, blocking, logging, and security alerts/escalation of unauthorized access requests

System Integrity

Systems should:

- Safeguard data by detecting and removing malware and other destructive software coding at network ingress and egress points, end-point mobile devices, desktops, servers, and storage devices
- Establish and enforce firewall and network perimeter security controls
- Ensure baseline data versioning, change management, and patching
- Acknowledge the success or failure of data transfers and maintain logging and reporting capabilities for data transfer events
- Ensure time stamps are captured and verifiable in an electronic forensic investigation

Physical Security

Systems processing or storing sensitive data should comply with the standards set forth in the most recent version of the MISMO eMortgage Vaulting Guide. The MISMO eMortgage Vaulting Guide provides details on industry-standard access control, surveillance, fire suppression, water detection, and natural disasters/hazards (e.g., earthquakes, hurricanes, tornados, tsunamis, floods, mudslides, landslides, etc.)

Systems should use:

- Physical access devices (e.g., keys, locks, combinations, card readers) and/or security guards
- Discreet building signage
- Building entrances and exits that are monitored for unauthorized access and activities
- At least two forms of authentication for entry of authorized staff to the data center, such as photo ID scan card and either a biometric device (finger print scanner, face recognition, etc.) or a number keypad
- Restrict visitor access requiring escorts and monitoring of their activities on premise
- Automatic emergency lighting that activates in the event of a power outage or disruption

- Fire suppression and detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire
- Master water shutoff valves that are accessible and working properly

Backup/Business Continuity

Systems processing or storing sensitive data should prevent the loss of data or access to data in the event of a system, facility, or data failure.

The system should:

- Store at least two backup copies of loan documents at all times
- Ensure that business units, data centers and applications and technology stacks are recoverable in the event of disaster
- Perform regular backups of all electronic records and restore electronic records that are damaged, corrupted, or lost
- Have at least one disaster recovery site which is physically separated from the primary location to prevent risks to availability of data caused by regional disasters
- Test business continuity/disaster recovery plans at least annually to ensure compliance with recovery time objectives/recovery point objectives