Members Exchange Federal Credit Union
Policies and Procedures

Policy: Information Security Policy – REVISED POLICY

Applies to: All Departments

Last Revision: July 31, 2025

Approved: April 30, 2026

Purpose
This policy establishes the governance framework for Members Exchange Federal Credit Union's (MEFCU) Information Security Program and defines the principles, responsibilities, and oversight necessary to manage information security risk and safeguard sensitive member information. The program supports compliance with applicable regulatory expectations, including guidance issued by the National Credit Union Administration and the Federal Financial Institutions Examination Council, as well as other applicable laws and regulations. The Board of Directors provides oversight and ensures that management implements appropriate administrative, technical, and physical safeguards to protect member information and critical systems.

Scope
This policy applies to all information systems, networks, applications, devices, and data owned, operated, or managed by Members Exchange Federal Credit Union (MEFCU), regardless of whether those resources are located on premises, hosted in cloud environments, or managed by third-party service providers.

This policy applies to:

- All MEFCU employees
- Contractors and temporary personnel
- Third-party service providers with access to MEFCU systems or data
- All workforce members who access or process MEFCU information

This policy governs the protection of all MEFCU information assets, including but not limited to:

- Member information and personally identifiable information (PII)
- Financial and transactional data
- Internal business information
- Systems, applications, and infrastructure supporting credit union operations

All workforce members and authorized users must comply with this policy, and the supporting security policies and procedures established under the MEFCU Information Security Program.

Information Security Objectives
Members Exchange Federal Credit Union maintains an Information Security Program designed to protect the confidentiality, integrity, and availability of information and information systems that support credit union operations and member services, including the protection of member information in accordance with applicable regulatory requirements. The Information Security Program supports the following security objectives:

Confidentiality
Protect sensitive information, including member information and internal business data, from unauthorized access, disclosure, or misuse.

Integrity
Ensure the accuracy, completeness, and reliability of information and systems by protecting them from unauthorized modification or destruction.

Availability
Ensure that critical systems and information remain accessible to authorized users when needed to support credit union operations and member services.

Accountability
Maintain appropriate logging, monitoring, and oversight mechanisms to ensure that actions affecting MEFCU systems and information can be traced to authorized individuals or processes. These objectives guide the design and implementation of administrative, technical, and physical safeguards within the Information Security Program.

Governance and Responsibilities
Effective information security requires clear governance, oversight, and accountability. MEFCU assigns responsibilities for the Information Security Program to ensure that information security risks are appropriately managed and that safeguards protecting member information and critical systems are maintained.

Board of Directors
The Board of Directors provides oversight of the Information Security Program and is responsible for approving this Information Security Policy. The Board ensures that management maintains an effective security program designed to protect member information and information systems in accordance with regulatory expectations. The Board receives periodic reporting regarding the status of the Information Security Program, including significant risks, security incidents, and the effectiveness of security controls.

Executive Management
Executive management is responsible for implementing and maintaining the Information Security Program and ensuring that appropriate administrative, technical, and physical safeguards are in place.

Responsibilities include:
- Supporting the implementation of information security policies and procedures
- Ensuring adequate resources for the security program
- Addressing risks identified through assessments or monitoring
- Promoting a culture of security awareness

Chief Information Officer and Senior Vice President-Risk Management
The Chief Information Officer (CIO) and the Senior Vice President – Risk Management are responsible for overseeing and coordinating the Information Security Program.

Responsibilities include:
- Overseeing the development and maintenance of information security policies, standards, and procedures
- Monitoring the effectiveness of security controls
- Coordinating information security risk assessment activities

- Reporting information on security matters to executive management and the Board of Directors
- Coordinating response activities related to information security incidents
- Supporting regulatory examinations and audit reviews related to information security

The CIO or SVP – Risk Management may delegate operational security responsibilities to qualified personnel or third-party service providers as necessary to support the effective operation of the Information Security Program.

Information Technology
The Information Technology function is responsible for implementing and maintaining technical security controls that support the Information Security Program.

Responsibilities include:
- Secure configuration and administration of systems and networks
- Monitoring system activity and responding to operational security events
- Implementing technical safeguards to protect systems and data
- Supporting vulnerability remediation and system maintenance activities

System and Data Owners
System and data owners are responsible for ensuring that systems and information within their areas of responsibility are protected in accordance with MEFCU policies and security standards.

Responsibilities include:
- Authorizing appropriate access to systems or information
- Supporting data protection and classification practices
- Ensuring systems are used in accordance with business and regulatory requirements

Workforce Members
All workforce members share responsibility for protecting MEFCU information and systems. Workforce members are expected to follow established security policies and procedures and promptly report suspected security incidents, phishing attempts, or other suspicious activity.

Detailed user responsibilities are defined in the **Acceptable Use Policy**.

Risk Management
MEFCU manages information security risk through a risk-based program that identifies, assesses, and mitigates threats to systems and member information. Risk assessments are conducted periodically and consider internal and external threats, technological changes, business processes, and regulatory expectations. Safeguards are implemented based on the organization's risk profile, and controls are periodically evaluated to ensure continued effectiveness. The Information Security Program includes periodic independent testing, such as internal or external audits, vulnerability assessments, and penetration testing, to validate the effectiveness of security controls. MEFCU also considers evolving threats, including emerging cyber risks and geopolitical factors, and adjusts its risk management activities accordingly.

Asset and Data Protection
MEFCU maintains safeguards to ensure that information assets and data are identified, classified, and protected based on sensitivity, criticality, and regulatory requirements. Inventories of systems, applications, infrastructure, and data repositories are maintained, and access to these assets is restricted based on business need. Policies and standards define requirements for data handling, retention, and secure disposal.

Physical Safeguards
Sensitive information in physical form must be protected from unauthorized access. Workforce members are responsible for securing documents, workstations, and devices when not in use and ensuring that sensitive information is stored and disposed of using approved methods.

Access Control and Identity Management
MEFCU restricts access to systems and data based on business needs and least privilege. Access must be approved through established processes, periodically reviewed, and promptly revoked when no longer required. Authentication mechanisms appropriate to system risk are used to verify user identity. Detailed requirements are defined in the **Access Control and Identity Management Policy**.

System and Network Security
MEFCU maintains safeguards to ensure the secure configuration, operation, and monitoring of systems, networks, and applications. Controls are implemented to reduce the risk of unauthorized access, misuse, or disruption, particularly for internet-facing systems and external access points. Operational security measures include configuration management, activity monitoring, and protection against unauthorized activity. Additional verification controls may be required for high-risk transactions.

Wireless Network Security
Wireless networks must be secured using appropriate authentication, encryption, and access controls. Only authorized wireless networks and devices may connect to MEFCU systems, and unauthorized access points are prohibited. Wireless activity may be monitored to ensure compliance with security requirements.

Email and Internet Security
MEFCU implements safeguards to reduce risks associated with email and internet usage, including protection against phishing, malicious websites, and unauthorized communications. Workforce members must comply with acceptable use requirements, and technical protections are enforced through security controls and supporting standards. Email and internet usage by workforce members must comply with the behavioral expectations defined in the **Acceptable Use Policy**.

Malware Protection
MEFCU maintains controls to prevent, detect, and respond to malware and other malicious software. Protective measures include endpoint security technologies, monitoring capabilities, and system safeguards appropriate to risk. Workforce members must not disable or circumvent these protections.

Vulnerability Management
MEFCU maintains processes to identify, evaluate, and remediate vulnerabilities through activities such as scanning, patch management, and system assessments. Systems are maintained with current updates, and remediation efforts are prioritized based on risk and potential impact. Detailed requirements are defined in the **Vulnerability Management Policy**.

Security Monitoring and Logging
MEFCU maintains logging and monitoring capabilities to detect security events, support investigations, and ensure accountability. System activity is monitored for anomalies, unauthorized access attempts, and indicators of compromise, with priority given to internet-facing systems and critical assets. Suspicious activity is escalated for further investigation.

Incident Management
MEFCU maintains procedures designed to identify, report, assess, contain, investigate, and recover from information security incidents. Workforce members are expected to promptly report suspected security incidents, including phishing attempts, unauthorized access, lost devices, or other suspicious activity. Incident management procedures establish escalation paths and responsibilities for responding to security

events, and significant incidents may be escalated to executive management and reported to the Board of Directors when appropriate. Where required by law or regulation, notifications may be made to regulatory authorities, law enforcement agencies, or affected individuals. Incident response procedures, including escalation, containment, and reporting requirements, are defined in the **Incident Response Plan** and supporting procedures.

MEFCU maintains procedures to evaluate and respond to potential data breach claims, unauthorized access events, or reports of compromise, including unverified claims. Response activities include coordination between technical, operational, legal, and communication functions as appropriate. MEFCU also maintains procedures to comply with regulatory reporting requirements, including notification to the National Credit Union Administration within required timeframes for reportable cyber incidents.

Business Continuity and Disaster Recovery
MEFCU maintains business continuity and disaster recovery capabilities designed to support the restoration of critical systems and services following operational disruptions or security incidents. Backup and recovery mechanisms are implemented to restore systems and data necessary to maintain operations and protect member information, and related procedures are periodically tested and reviewed to ensure effectiveness. Backup and recovery strategies include protections to prevent unauthorized alteration, deletion, or encryption of critical data, and restoration capabilities are regularly tested to ensure operational resilience and the ability to restore critical services within acceptable timeframes. Detailed recovery procedures are defined in the **Emergency Preparedness & Disaster Recovery Policy (BCDR)**.

Vendor and Third-Party Risk Management
MEFCU manages risks associated with third-party service providers that access, process, store, or transmit MEFCU information or support critical credit union operations. Vendor risk management processes include due diligence, contractual security requirements, and ongoing oversight of vendor security practices, and third-party providers are expected to maintain safeguards appropriate to the sensitivity of the information and services provided. MEFCU considers third-party risks as part of its overall threat environment, including supply chain disruptions, service provider compromise, and external dependencies. Vendor risk management requirements, including due diligence, contractual controls, and ongoing monitoring, are defined in the **Vendor and Third-Party Risk Management Policy** and supporting procedures.

Security Awareness and Training
MEFCU provides ongoing information security awareness training to ensure that workforce members understand their responsibilities for protecting systems and information. Training reinforces recognition of phishing, social engineering, and other evolving threats, and may include simulated exercises and targeted training for higher-risk roles.

Exceptions
Exceptions to this policy must be documented, evaluated for risk, and approved by authorized management. Approved exceptions must include appropriate compensating controls and review timelines to ensure that risks remain appropriately managed.

Enforcement
Violations of this policy may result in disciplinary action in accordance with MEFCU personnel policies and procedures. Disciplinary actions may include corrective measures, suspension of system access, or termination of employment or contractual relationships where appropriate. Security incidents involving potential violations may be investigated in accordance with incident response procedures.

Supporting Policies
This Information Security Policy establishes the framework for the Members Exchange Federal Credit Union (MEFCU) Information Security Program. Supporting policies and standards provide more detailed requirements governing specific aspects of information security, system use, and operational security controls.

These supporting policies include, but are not limited to:

- **Acceptable Use Policy**
- **Incident Response Plan**
- **Emergency Preparedness and Disaster Recovery Policy**
- **Physical Security Policy**
- **Password Policy**
- **Confidentiality of Accounts Policy**
- **Portable Device Security Policy**
- **Vendor and Third-Party Risk Management Policy**

These supporting documents may be maintained and updated through management processes without requiring Board re-approval, provided such updates do not materially alter the intent of this Information Security Policy.

Approval
This Information Security Policy is approved by the Board of Directors and forms part of the Members Exchange Federal Credit Union Information Security Program.

Management is responsible for implementing and maintaining this policy and presenting revisions to the Board of Directors when substantive changes are required.

Program Review and Reporting
The Members Exchange Federal Credit Union Information Security Program is subject to periodic review to ensure that safeguards remain effective and appropriate for the organization's risk environment.

The Chief Information Officer or Senior Vice President-Risk Management provides periodic reporting to executive management and the Board of Directors regarding the status of the Information Security Program. These reports may include information regarding:

- significant information security risks
- security incidents and response activities
- the effectiveness of security controls
- results of risk assessments, testing, or audits

The Information Security Program may be updated as necessary to address changes in technology, operational requirements, regulatory expectations, or the evolving threat landscape. Reporting may incorporate relevant threat intelligence and external advisories to support informed risk management and decision-making.

This policy was approved at a regularly scheduled Board of Directors meeting on April 30, 2026. The Online Boardroom and Board of Directors' meeting minutes document the approval.