Purpose

The purpose of this policy is to establish robust identity and access management (IAM) practices to protect Maple Trust Credit Union's information systems, member data, and physical infrastructure. This policy aligns with NIST Cybersecurity Framework (CSF) requirements to enhance security, reduce risks, and ensure operational continuity.

Scope

This policy applies to all employees, contractors, vendors, and third-party entities who access Maple Trust Credit Union's systems, applications, data, and physical facilities.

Policy Statements

All users, systems, and devices must be uniquely identified through robust identity verification processes before access is granted to any organizational resources.

Multi-factor authentication (MFA) is required for all users accessing critical systems, sensitive member data, and remote access points.

Access permissions shall follow the principle of least privilege, granting users the minimum access required to perform their job responsibilities.

Access permissions must be reviewed at least quarterly to ensure alignment with current job roles and responsibilities. Privileged accounts must be reviewed monthly for appropriateness and proper use.

Inactive accounts will be automatically disabled after 30 days unless specifically authorized for extension. User accounts for terminated or transferred employees must be deactivated immediately.

Physical access to facilities and sensitive areas, including data centers, must be controlled through badges, biometrics, or equivalent mechanisms and monitored through logs and video surveillance.

All access events, including successful and failed login attempts, privilege escalations, and account modifications, must be logged and monitored. Anomalous activity must trigger automated alerts for investigation.

Access logs shall be retained for a minimum of one year and reviewed quarterly to detect unauthorized access or policy violations.

Third-party access must adhere to Maple Trust Credit Union's IAM policies. Third-party accounts must be limited to the minimum access required and terminated immediately upon the conclusion of their engagement.

Employees and contractors must complete annual IAM training, including secure password creation, phishing awareness, and understanding their access-related responsibilities. Privileged users must undergo specialized training on secure management practices.

Compromised credentials must be deactivated immediately upon detection. Users affected by compromised credentials must undergo identity revalidation before access is reinstated.

IAM processes and tools must be reviewed annually to ensure alignment with NIST CSF and emerging security threats. Regular audits will be conducted to assess IAM effectiveness and identify areas for improvement.

Real-time monitoring tools shall be employed to detect suspicious activity related to identity and access management, including unauthorized attempts to escalate privileges or access sensitive systems.

The IAM administrator is responsible for maintaining and enforcing the IAM processes, systems, and tools. Managers are responsible for ensuring their team members' access aligns with their roles, and all employees must adhere to IAM policies and report suspicious activity.

Non-compliance with this policy may result in disciplinary actions, including termination of access or employment. Maple Trust Credit Union reserves the right to audit access and investigate violations.

Review and Updates

This policy will be reviewed annually and updated to address emerging threats and ensure continued compliance with NIST Cybersecurity Framework requirements.