Employee and HR Policy

Purpose

The purpose of this policy is to establish guidelines for managing employee conduct, roles, and responsibilities to safeguard Maple Trust Credit Union's operations, data, and reputation. It aligns with NIST Cybersecurity Framework (CSF) principles to promote a secure and compliant work environment.

Scope

This policy applies to all employees, contractors, interns, and temporary staff at Maple Trust Credit Union.

Policy Statements

Hiring and Onboarding

All prospective employees must undergo a thorough background check, including identity verification, employment history, and, where applicable, criminal and financial checks.
New employees must sign confidentiality agreements and acknowledge Maple Trust Credit Union's code of conduct, cybersecurity policies, and acceptable use guidelines.
Role-specific security training must be completed within the first 30 days of employment.

Roles and Responsibilities

All employees are responsible for adhering to Maple Trust Credit Union's cybersecurity and data protection policies.
Supervisors must ensure their team members comply with security policies, complete required training, and have access only to systems and data necessary for their roles.
The HR department is responsible for maintaining employee records, conducting periodic policy reviews, and addressing non-compliance.

Acceptable Use

Employees must use Maple Trust Credit Union's systems, devices, and resources only for authorized business purposes.

Personal use of organizational resources is limited and must not interfere with work responsibilities or security.
The use of unauthorized software, hardware, or cloud services is prohibited.

Security Awareness and Training
Employees must complete annual security awareness training, including modules on phishing, password management, and secure data handling.
Employees with privileged access must undergo additional role-specific training on secure system management and incident response.

Access Control
Access to systems, data, and facilities must follow the principle of least privilege and align with the employee's role.
Multi-factor authentication (MFA) is required for access to critical systems and sensitive data.
Employee access rights must be reviewed quarterly and updated to reflect role changes, promotions, or terminations.

Remote Work
Employees working remotely must use approved devices and secure connections, such as a VPN.
Confidential or restricted data must not be stored or processed on personal devices without prior approval.
Home office environments must meet minimum security requirements, including antivirus software and firewalls.

Disciplinary Action and Non-Compliance
Failure to comply with this policy or other organizational policies may result in disciplinary action, including termination of employment.
Significant violations, such as unauthorized data access or sharing, may be referred to legal authorities.

Termination and Offboarding
Upon termination of employment, all access to systems, devices, and facilities must be revoked immediately.
Employees must return all organizational property, including devices, ID badges, and access tokens, on or before their last working day.

Exit interviews must include reminders of confidentiality agreements and policies governing the use of organizational data post-employment.

Data Protection and Privacy
Employees must handle all sensitive member or employee data in compliance with data privacy policies and applicable regulations (e.g., GDPR, CCPA).
Any unauthorized access, sharing, or disclosure of data is strictly prohibited and must be reported immediately.

Incident Reporting
Employees must report any suspected security incidents, including phishing attempts, data breaches, or unauthorized access, to the IT or security team immediately.
Reports of incidents must be documented and addressed promptly to minimize potential impacts.

Diversity, Equity, and Inclusion (DEI)
Maple Trust Credit Union is committed to fostering a diverse, equitable, and inclusive workplace.
Employees are expected to treat colleagues, customers, and partners with respect and professionalism, regardless of race, gender, ethnicity, religion, or background.

Health and Safety
Maple Trust Credit Union is committed to maintaining a safe and healthy workplace. Employees must adhere to all health and safety policies and report any hazards or unsafe conditions promptly.

Roles and Responsibilities
The **HR Department** is responsible for policy implementation, training coordination, and addressing employee-related issues.
Supervisors must ensure their teams adhere to policies and report non-compliance.
Employees must understand and comply with all HR and organizational policies.

Review and Updates

This policy must be reviewed annually and updated to reflect changes in regulations, organizational priorities, or the threat landscape.

Compliance
Non-compliance with this policy may result in disciplinary actions, up to and including termination of employment.