Data Management Policy

Purpose

This policy establishes guidelines for the governance, classification, handling, retention, and protection of data at Maple Trust Credit Union. It aims to safeguard sensitive data, ensure regulatory compliance, and support the organization’s strategic goals in alignment with the NIST Cybersecurity Framework (CSF).

Scope

This policy applies to all data created, collected, stored, processed, or transmitted by Maple Trust Credit Union, including data handled by employees, contractors, and third-party vendors.

Policy Statements

Data Governance

A centralized data governance framework must be implemented to oversee data management practices, ensuring data accuracy, integrity, and security. A Data Governance Committee shall be established to oversee adherence to this policy and address emerging data management requirements. Ownership of all data must be assigned to specific business units, with data stewards responsible for ensuring compliance with data classification, retention, and protection requirements.

Data Classification

All data must be classified into one of the following categories based on its sensitivity and impact level:

1. **Public**: Data intended for public dissemination, such as marketing materials.
2. **Internal**: Data used within the organization, such as policies and operational documents.
3. **Confidential**: Sensitive data requiring limited access, such as employee or vendor records.
4. **Restricted**: Highly sensitive data requiring strict access controls, such as member financial information.

Data classification levels must be reviewed annually or when significant changes occur.

Data Handling

Access to data must follow the principle of least privilege, ensuring users only access data necessary for their roles.

Confidential and restricted data must be encrypted during transmission (e.g., using TLS) and at rest (e.g., using AES-256).

Sensitive data must not be stored on personal devices or unauthorized storage systems.

When sharing data externally, all transfers must be approved, encrypted, and logged.

Data Retention and Disposal

Retention schedules must be established for all data types to comply with regulatory and operational requirements.

Data no longer needed for business or compliance purposes must be securely disposed of using approved methods, such as shredding for physical records or secure deletion for digital files.

Data retention schedules and disposal practices must be reviewed annually to ensure compliance with legal and business requirements.

Data Protection

Access to data must be managed using robust authentication mechanisms, including multi-factor authentication (MFA) for sensitive systems.

Data backups must be performed regularly, with backup copies stored in secure, geographically diverse locations to support disaster recovery efforts.

Data loss prevention (DLP) tools must be employed to monitor and control unauthorized data access, sharing, or exfiltration.

Monitoring and Audit

All access to sensitive data must be logged and monitored for anomalies, including unauthorized access attempts and data breaches.

Audit logs must be retained for a minimum of one year and reviewed quarterly to identify potential policy violations or risks.

Regular audits of data management practices must be conducted to ensure alignment with this policy and NIST CSF requirements.

Training and Awareness

Employees, contractors, and third-party vendors must receive annual training on data classification, handling, and protection practices.
Specialized training must be provided to data stewards and users handling restricted data.

Incident Response

In the event of a suspected or confirmed data breach, the incident response team must be activated immediately to mitigate impacts, notify stakeholders, and restore data integrity.
All data breaches must be documented, reviewed, and reported in accordance with regulatory requirements.

Roles and Responsibilities

The **Data Governance Committee** is responsible for implementing and maintaining this policy.
Data Stewards are responsible for ensuring compliance with data classification, retention, and handling guidelines.
Employees and Contractors are responsible for adhering to data handling and protection requirements outlined in this policy.

Review and Updates

This policy must be reviewed and updated annually or as necessary to address changes in regulations, business requirements, or the threat landscape.

Compliance

Non-compliance with this policy may result in disciplinary action, including termination of access or employment, and contractual penalties for third-party vendors.