Third-Party Vendor Management Policy

Purpose

This policy establishes a framework for managing third-party vendors to ensure their services meet Maple Trust Credit Union's security, compliance, and operational standards. The policy aligns with NIST Cybersecurity Framework (CSF) principles to protect organizational data, systems, and reputation.

Scope

This policy applies to all third-party vendors, contractors, service providers, and consultants who access, process, store, or transmit Maple Trust Credit Union's data or interact with its systems.

Policy Statements

Vendor Selection and Risk Assessment

All vendors must undergo a risk assessment before engagement to evaluate their cybersecurity practices, financial stability, and compliance with regulatory requirements.

Vendors handling sensitive or critical data must demonstrate adherence to recognized security frameworks, such as ISO 27001, SOC 2, or NIST CSF.

High-risk vendors must undergo additional due diligence, including on-site audits or penetration testing, as deemed necessary.

Contractual Requirements

All vendor agreements must include:

- Defined roles and responsibilities for security and data protection.
- Confidentiality clauses to protect sensitive information.
- Breach notification requirements with clear timelines for reporting incidents.
- Provisions for compliance with applicable regulations (e.g., GDPR, CCPA, PCI DSS).

Vendors must agree to periodic security assessments or audits as part of the contract terms.

Access Control
Vendors must be granted the minimum level of access necessary to perform their duties, following the principle of least privilege.
Access to Maple Trust Credit Union's systems must be monitored and logged, and inactive vendor accounts must be disabled after 30 days of inactivity.
Multi-factor authentication (MFA) is required for vendor access to sensitive systems or data.

Data Protection
Vendors must encrypt all sensitive data during transmission (e.g., TLS) and at rest (e.g., AES-256).
No sensitive data may be stored on unapproved devices or systems without explicit authorization.
Data shared with vendors must be limited to what is necessary for their services and sanitized where possible.

Monitoring and Auditing
Vendor activity must be logged and monitored to detect unauthorized access, data exfiltration, or policy violations.
Audits of high-risk vendors must be conducted annually to verify compliance with contractual security requirements.
Incident trends involving vendors must be analyzed quarterly to identify and mitigate systemic risks.

Incident Response and Reporting
Vendors must report any security incident or data breach immediately upon discovery.
Maple Trust Credit Union reserves the right to suspend or terminate vendor access during incident investigations.
Post-incident reviews must be conducted to evaluate the root cause, impact, and corrective actions taken by the vendor.

Termination and Offboarding
Upon contract termination, all vendor access to systems and data must be revoked, and a confirmation of data destruction must be obtained.
Terminated vendors must return or securely delete any Maple Trust Credit Union data within 30 days.

Training and Awareness

Vendors must receive training on Maple Trust Credit Union's security policies and standards, tailored to their level of interaction with the organization's systems or data.
Specialized training must be provided to vendors handling sensitive data or operating critical systems.

Roles and Responsibilities

The **Vendor Management Team** is responsible for evaluating, onboarding, and monitoring vendor compliance with this policy.
The **Risk and Compliance Team** is responsible for conducting risk assessments and audits of third-party vendors.
All **Employees** interacting with vendors must ensure compliance with this policy and report any suspected violations.

Review and Updates

This policy must be reviewed and updated annually or in response to changes in regulatory requirements, business operations, or the threat landscape.

Compliance

Non-compliance with this policy by vendors or employees may result in termination of contracts, access, or employment, as well as potential legal or financial penalties.