Encryption Policy for Maple Trust Credit Union

1. **Policy Title: Encryption Policy**

Effective Date: [Insert Date]
Approved By: Chief Executive Officer (Alexandra Grant)
Owner: Chief Information Security Officer (CISO) - Jordan West
Applies To: All employees, contractors, vendors, and third parties with access to the organization's data, devices, and information systems.

2. **Purpose**

The purpose of this policy is to ensure that all sensitive data at Maple Trust Credit Union is encrypted to protect against unauthorized access, data breaches, and regulatory violations. This policy defines the minimum encryption standards and procedures for data at rest, data in transit, and encryption key management. The policy supports compliance with **OSFI**, **PCI DSS**, **PIPEDA**, and other applicable regulatory frameworks.

3. **Scope**

This policy applies to all data, systems, and personnel that access or handle sensitive information, including but not limited to:

- Customer data, financial data, payment card data, and employee data
- Devices such as laptops, desktops, servers, mobile devices, and USB drives
- Internal systems, cloud systems, and third-party services where data is stored, transmitted, or processed

4. **Roles and Responsibilities**

- **Chief Information Security Officer (CISO)**: Oversees the implementation, monitoring, and enforcement of the Encryption Policy.
- **IT Department**: Implements encryption technology, manages key lifecycle, and ensures encryption compliance.
- **Employees and Contractors**: Ensure compliance with encryption requirements when handling sensitive data.
- **Internal Audit Department**: Conducts quarterly audits to assess compliance with the Encryption Policy.

5. **Policy Statements**

5.1 Data at Rest

- All **data at rest** on endpoints (laptops, desktops, mobile devices) must be encrypted using **AES-256 encryption**.
- Servers, virtual machines, and cloud storage (e.g., AWS, Azure) must have encryption enabled for all data at rest.
- Removable media, such as USB drives, must be encrypted before use on the corporate network.
- Databases containing sensitive information must use **Transparent Data Encryption (TDE)** or equivalent database encryption.

5.2 Data in Transit

- All **data in transit** between users, systems, and external services must be encrypted using **TLS 1.2 or higher**.
- **Email communication** containing sensitive information must be encrypted using **Secure/Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy (PGP)**.
- **Web-based applications** that transmit sensitive data (e.g., customer portals) must use **HTTPS**.
- **VPNs** must be used to encrypt traffic for remote access to the internal network.

5.3 Key Management

- **Encryption keys** must be managed using a **Key Management System (KMS)** with strong controls for key generation, storage, distribution, rotation, and destruction.
- Keys must be rotated annually or after a security incident.
- Encryption keys must be stored in a **Hardware Security Module (HSM)** or in a secure **Cloud Key Management Service (e.g., AWS KMS, Azure Key Vault)**.
- Key access must be limited to **authorized personnel only**, and logs must be maintained for all key access activities.

5.4 Endpoint Encryption

- Full-disk encryption (FDE) must be applied to all employee devices, including laptops, desktops, and mobile devices.
- **Mobile Device Management (MDM)** is required to enforce encryption for smartphones and tablets.
- Devices that do not comply with this policy will be denied access to corporate systems and networks.

5.5 Cloud Encryption

- All data stored in **cloud services (e.g., AWS, Azure, GCP)** must be encrypted using **AES-256**.
- Cloud providers must support **bring your own key (BYOK)** or **customer-managed keys (CMK)** to allow Maple Trust Credit Union to retain control of encryption keys.
- **Object storage (e.g., AWS S3, Azure Blob Storage)** must be encrypted at the bucket level using **server-side encryption (SSE)**.

5.6 Application-Level Encryption

- Sensitive data stored in applications (e.g., customer information, payment card data) must be encrypted at the application level using **field-level encryption**.
- Payment data must be encrypted in compliance with **PCI DSS requirements**.
- **Tokenization** may be used as an alternative to encryption where appropriate.

5.7 Encryption for Backups

- Backups of sensitive data must be encrypted using **AES-256 encryption** before being stored.
- Backup storage systems must enforce encryption for data at rest.
- Backup keys must be stored securely in a **Key Management System (KMS)** and rotated annually.

5.8 Monitoring and Logging

- Access to encryption keys and encrypted data must be **logged and monitored** using **Security Information and Event Management (SIEM)** tools.
- Alerts must be triggered for **unauthorized access attempts** on encryption keys and encrypted data.
- Logs must be retained for **12 months** to support compliance audits and investigations.

5.9 Compliance and Audits

- Compliance with the Encryption Policy will be audited quarterly by the **Internal Audit Department**.
- **External audits** will be conducted annually to ensure compliance with **PCI DSS, OSFI, and PIPEDA**.
- Failure to comply with this policy may result in **disciplinary action**, up to and including **termination of employment**.

6. **Exceptions**

Any requests for exceptions to this policy must be submitted to the **Chief Information Security Officer (CISO)** for review and approval. Exceptions must be documented, including the reason for the exception and the compensating controls in place.

7. **Policy Review**

This policy will be reviewed annually or as required by changes in **regulatory compliance, technology, or threat landscape**.

8. **Approval and Review**

This policy has been reviewed and approved by:

- **Chief Executive Officer (CEO)**: Alexandra Grant
- **Chief Information Security Officer (CISO)**: Jordan West