IT Security Policy for Maple Trust Credit Union

1. Policy Title: IT Security 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 information systems.

2. Purpose

The purpose of this policy is to ensure the confidentiality, integrity, and availability of Maple Trust Credit Union’s information systems and to protect the organization from cybersecurity threats, data breaches, and operational disruptions. This policy establishes guidelines for access control, data protection, incident response, and network security in compliance with OSFI, PCI DSS, PIPEDA, and other applicable regulatory standards.

3. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to Maple Trust Credit Union’s information technology (IT) resources, including but not limited to:

- Physical Devices: Laptops, desktops, mobile devices, USB drives, and removable media.
- IT Systems: Servers, databases, file storage, and network infrastructure.
- Cloud Systems: SaaS, PaaS, and IaaS services (e.g., AWS, Azure, GCP).
- Data: Customer data, financial data, intellectual property, and employee information.

4. Roles and Responsibilities

- Chief Information Security Officer (CISO): Oversees the implementation and monitoring of the IT Security Policy.
- IT Department: Ensures compliance with the policy, performs vulnerability scans, and manages IT infrastructure.
- Employees and Contractors: Adhere to the security protocols defined in this policy.
- Internal Audit Department: Conducts audits to ensure compliance with the policy.

5. Policy Statements

5.1 Access Control

- All users must have unique user IDs and strong passwords (minimum of 12 characters) for system access.
- Multi-Factor Authentication (MFA) must be used for all remote access and administrative accounts.
- Access to sensitive data is granted on a “least privilege” basis.

5.2 Data Protection

- Data at rest must be encrypted using AES-256 encryption.
- Data in transit must be encrypted using TLS 1.2 or higher.
- Backups must be taken daily and stored in a secure offsite location.

5.3 Network Security

- Firewalls must be configured to block unauthorized access to the network.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) must be deployed to detect and block malicious activity.
- Wi-Fi networks must be secured with WPA3 encryption.

5.4 Device and Endpoint Security

- All devices (laptops, desktops, mobile devices) must have endpoint protection and antivirus software installed.
- USB drives and removable media must be encrypted before use.
- Mobile device management (MDM) must be used to secure employee smartphones and tablets.

5.5 Incident Response

- All security incidents must be reported immediately to the Incident Response Team (IRT) via the incident hotline.
- Incident response procedures must be tested at least once per year via tabletop exercises.
- Breaches involving customer data must be reported to regulators (e.g., OSFI) within 72 hours.

6. Compliance and Audits

- Internal audits will be conducted quarterly by the Internal Audit Department to assess compliance with this policy.
- External audits will be conducted annually to ensure compliance with PCI DSS, OSFI, and PIPEDA regulations.
- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.

7. Exceptions

Any requests for exceptions to this policy must be submitted in writing to the Chief Information Security Officer (CISO) for review and approval.

8. Policy Review

This policy will be reviewed annually or as required by regulatory changes or changes in business operations.

9. Approval and Review

This policy has been reviewed and approved by:

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