Network Security Policy for Maple Trust Credit Union

1. **Policy Title: Network 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 network and information systems.

2. **Purpose**

The purpose of this policy is to establish a secure network environment for Maple Trust Credit Union. The goal is to protect the network from unauthorized access, cyberattacks, data breaches, and service disruptions. This policy outlines the controls and practices required to ensure the confidentiality, integrity, and availability of the organization's network infrastructure.

3. **Scope**

This policy applies to all individuals with access to Maple Trust Credit Union's network, including employees, contractors, third-party vendors, and any device or system connected to the network. The scope includes, but is not limited to:

- Firewalls, routers, and network switches
- Wireless Access Points (WAPs) and Wi-Fi networks
- Virtual Private Networks (VPNs)
- Internal and external networks, cloud networks, and remote connections
- Connected devices, such as laptops, desktops, servers, mobile devices, and IoT devices

4. **Roles and Responsibilities**

- **Chief Information Security Officer (CISO)**: Oversees the implementation and enforcement of the Network Security Policy.
- **IT Department**: Manages the configuration and maintenance of firewalls, VPNs, IDS/IPS, and network security controls.
- **Employees and Contractors**: Adhere to the security protocols and use the network in a manner consistent with this policy.
- **Internal Audit Department**: Conducts periodic audits to ensure compliance with network security standards.

5. **Policy Statements**

5.1 Access Control

- Access to the network is limited to authorized users only.
- All users must authenticate using **Multi-Factor Authentication (MFA)** when accessing the network remotely.
- Users are assigned access based on the principle of **least privilege**, and access is reviewed quarterly.
- Access to network devices (e.g., firewalls, routers, and switches) is restricted to authorized network administrators.

5.2 Firewall and Perimeter Security

- **Firewalls** must be configured to block unauthorized traffic and only allow necessary inbound and outbound traffic.
- Firewalls are updated regularly with the latest firmware and security patches.
- Firewall rules must be reviewed quarterly to ensure they adhere to the principle of "deny by default, allow by exception."
- Firewalls must log all traffic activity, and logs are retained for a minimum of **12 months**.

5.3 Intrusion Detection and Prevention (IDS/IPS)

- **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** must be deployed to detect and block malicious activity.
- Alerts generated by IDS/IPS must be monitored 24/7 by the Security Operations Center (SOC) team.
- Incident response procedures must be initiated within **15 minutes** of receiving a critical IDS/IPS alert.

5.4 Wi-Fi and Wireless Network Security

- All **Wi-Fi networks** must be secured using **WPA3 encryption**.
- Guest Wi-Fi networks must be segregated from the corporate network to prevent lateral movement of attacks.
- Devices must be required to authenticate using **MAC address filtering** for Wi-Fi access.
- Wireless Access Points (WAPs) must be managed through a centralized system with role-based access control.

5.5 VPN and Remote Access

- All remote users must connect via a **Virtual Private Network (VPN)** with end-to-end encryption.
- **Split tunneling** is disabled on the VPN to prevent data leakage.
- VPN access is granted only to employees and contractors with a business need for remote access.
- VPN access logs are retained for a period of **12 months**.

5.6 Device Security and Network Segmentation

- **Network segmentation** is used to separate critical systems from general-purpose systems.
- **Production, development, and testing environments** must be isolated from each other.
- Critical assets (e.g., payment systems, HR systems) must be placed on segmented VLANs with restricted access.
- IoT devices are isolated on a dedicated network segment to prevent unauthorized access.

5.7 Data Encryption and Transmission Security

- All data transmitted across the network must be encrypted using **TLS 1.2 or higher**.
- Endpoints accessing the network must be encrypted using **AES-256 encryption** for data at rest.
- Sensitive data (e.g., payment card data) is only transmitted over secure protocols such as **HTTPS, SFTP, and SSH**.

5.8 Logging and Monitoring

- Network logs, including **firewall logs, VPN logs, and IDS/IPS logs**, are collected and stored in a centralized logging system.
- Logs are retained for a minimum of **12 months** to support incident investigation and regulatory compliance.
- **Automated alerting** is configured to detect abnormal network activity, such as port scans, failed login attempts, and DDoS attacks.

5.9 Change Management

- All network changes (e.g., firewall rules, router configurations) must be approved through a formal **change management process**.

- Emergency changes must be documented and approved retroactively by the **Change Advisory Board (CAB)**.
- Changes must be tested in a staging environment before being applied to the production network.

5.10 Incident Response

- All network security incidents must be reported to the **Incident Response Team (IRT)** within **15 minutes** of discovery.
- Incident response procedures must be tested at least **annually** through **tabletop exercises**.
- Network incidents involving data breaches must be reported to regulators (e.g., **OSFI**) within **72 hours**.

6. Compliance and Audits

- The Internal Audit Department conducts quarterly audits to assess network security controls and identify areas for improvement.
- External audits are conducted annually to ensure compliance with **PCI DSS, OSFI, and PIPEDA**.
- **Non-compliance** with the Network Security Policy may result in disciplinary action, including termination of employment.

7. Exceptions

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

8. Policy Review

This policy will be reviewed **annually** or when significant changes occur in regulatory requirements, network infrastructure, or threat landscape.

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