Maple Trust Cybersecurity Policy

Introduction:

Maple Trust is a medium-sized organization dedicated to protecting the confidentiality, integrity, and availability of its information assets. This policy outlines our commitment to implementing baseline cybersecurity practices in line with the Canadian Centre for Cyber Security's recommendations for small and medium organizations.

Incident Response:

Maple Trust maintains a written incident response plan. This plan includes clear responsibilities, contact information for external parties, and procedures to manage various levels of cybersecurity incidents. A hard copy of the plan is kept off-network for emergency access.

Patching and Software Updates:

All organization systems are configured to receive automatic patches. Systems that cannot be updated automatically are reviewed periodically for manual updates or replacement.

Security Software and Firewalls:

We deploy anti-malware software with automatic updates and scans on all endpoint devices. Software firewalls are enabled on all systems unless an alternative enterprise firewall solution is documented.

Secure Configuration:

Default passwords are changed on all devices. Unnecessary features are disabled and critical security settings are enforced across the infrastructure.

User Authentication:

Multi-factor authentication (MFA) is required for sensitive systems including financial accounts, privileged access, and administrative portals. Passwords must meet complexity requirements and are changed upon suspected compromise.

Employee Awareness and Training:

All employees undergo mandatory cybersecurity awareness training covering secure practices, password hygiene, phishing awareness, and safe browsing habits.

Data Backup and Encryption:

Essential business systems are backed up regularly. Long-term backups are encrypted and stored offline. Access to backups is restricted and restoration procedures are tested semi-annually.

Mobile Devices:

Maple Trust uses a COPE (Company-Owned, Personally Enabled) model. Work and personal data are separated on mobile devices. Encryption is required and employees must install only approved apps.

Perimeter and Network Defenses:

Our network includes enterprise firewalls and DNS filtering to protect against malicious sites. Public and corporate networks are fully segregated. All remote access requires VPN with MFA.

Cloud and Outsourced IT Services:

Only vetted cloud vendors with SOC 3 compliance are used. Sensitive data is encrypted before cloud transmission. MFA is enforced for all administrative cloud accounts.

Website Security:

All Maple Trust websites are assessed against OWASP Top 10 vulnerabilities. Periodic security testing and updates are part of our development lifecycle.

Access Control:

User privileges follow the principle of least privilege. Accounts are deactivated immediately upon employment termination. Administrative accounts are restricted from user-level activities.

Portable Media:

Only organization-approved, encrypted portable media is permitted. Disposal includes secure data sanitization or certified destruction.

Conclusion:

This policy reflects Maple Trust's proactive approach to reducing cybersecurity risk and enhancing its digital resilience. Additional controls may be added over time to address evolving threats.