Purpose

The purpose of this policy is to establish a framework for maintaining and restoring business operations in the event of a disruption. This policy ensures the resilience of Maple Trust Credit Union's critical services, including safeguarding member data and financial operations, while complying with NIST Cybersecurity Framework (CSF) requirements.

Scope

This policy applies to all critical business functions, IT systems, employees, contractors, vendors, and facilities involved in the delivery of Maple Trust Credit Union's services.

Policy Statements

Maple Trust Credit Union shall maintain a comprehensive Business Continuity Plan (BCP) that identifies critical operations, assets, and dependencies essential to delivering uninterrupted services to members.

The BCP must include detailed procedures for responding to and recovering from various disruption scenarios, including natural disasters, cyberattacks, power outages, and pandemics.

A Business Impact Analysis (BIA) must be conducted annually to identify and prioritize critical systems, services, and processes based on their potential impact on members and stakeholders.

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) must be defined for all critical systems and processes to ensure timely recovery and minimal data loss.

Redundant systems and data backups must be maintained and tested regularly to ensure availability and integrity during recovery efforts.

Emergency contact information for key personnel, vendors, and partners must be documented and updated regularly to ensure effective communication during an incident.

The BCP must include clearly defined roles and responsibilities for incident response and recovery teams, including executive oversight, IT recovery leads, and communications coordinators.

Employees and contractors must be trained annually on their roles in the BCP to ensure preparedness and minimize downtime during a disruption.

Third-party vendors and service providers must adhere to Maple Trust Credit Union's BCP standards and provide evidence of their own business continuity plans.

All critical systems and facilities must be included in semi-annual BCP testing exercises, such as tabletop simulations, failover drills, and disaster recovery tests.

Incidents resulting in the activation of the BCP must be thoroughly documented and reviewed post-recovery to identify gaps and implement improvements.

The BCP must include a communication plan for notifying members, employees, regulators, and other stakeholders in the event of a disruption.

The BCP must be reviewed and updated annually or whenever significant changes occur to the business, technology, or threat landscape.

Compliance with this policy is mandatory, and non-adherence may result in disciplinary action or contractual penalties for third-party vendors.

Roles and Responsibilities

The Business Continuity Officer is responsible for developing, maintaining, and testing the BCP. Department heads must ensure their teams are prepared to execute BCP procedures, and all employees must adhere to their roles as defined in the plan.

Review and Updates

This policy will be reviewed annually and updated as necessary to reflect organizational changes, emerging threats, and evolving best practices.