Mentornity

Recovery Operations Policy

Purpose and Scope

This policy defines the procedures and actions to be taken by Mentornity to restore systems and operations to normalcy following a cybersecurity incident. This policy ensures that all necessary steps are planned and executed to recover from incidents with minimal impact on business operations and to maintain continuity.

Policy Components

1. **Recovery Planning (RC.RP - Recovery Planning)**
    - Mentornity has established a comprehensive **Recovery Plan** that provides a framework for rebuilding systems and resuming operations following a cybersecurity incident. The Recovery Plan consists of the following key elements:
        - **Risk Assessment and Impact Analysis:** Prior to recovery efforts, a thorough assessment is conducted to evaluate the extent of the damage, affected systems, and the impact on business operations.
        - **Recovery Prioritization:** Based on the impact analysis, critical systems and services are prioritized for recovery. A clear order of restoration is defined to ensure business continuity.
        - **Recovery Steps and Procedures:** Detailed recovery procedures are documented for different types of incidents (e.g., data breaches, ransomware attacks, system outages). These steps outline the actions needed to restore affected systems to a secure and operational state.
        - **Backup and Restoration Procedures:** Regular backups are maintained for all critical systems and data. The recovery plan includes specific instructions for restoring data from backups and verifying data integrity post-recovery.

        - **Recovery Roles and Responsibilities:** Clearly defined roles and responsibilities are assigned to team members involved in the recovery process, including IT staff, management, and external partners as needed.
2. **Continuous Improvement of Recovery Processes (RC.IM - Improvements)**
    - To ensure the effectiveness of the recovery processes, Mentornity commits to regular review and continuous improvement:
        - **Post-Recovery Review:** After each recovery operation, a comprehensive review is conducted to evaluate the effectiveness of the recovery efforts. Lessons learned are documented and shared with relevant teams.
        - **Updating the Recovery Plan:** Based on the findings from post-recovery reviews, the recovery plan is regularly updated to address any gaps or weaknesses identified during the recovery process.
        - **Regular Testing and Simulation:** The recovery plan is tested regularly through simulations and tabletop exercises to ensure preparedness for real incidents. These tests help in identifying potential improvements and validating recovery strategies.
3. **Communication During Recovery (RC.CO - Communications)**
    - Clear and transparent communication is essential during the recovery phase to keep stakeholders informed and maintain trust:
        - **Internal Communication:** A structured communication plan is in place to keep internal teams (e.g., IT, Legal, Public Relations, Management) updated on recovery progress and timelines.
        - **External Communication:** Clients, partners, and regulatory bodies are informed about the recovery status and any potential impact on their operations through predefined communication channels.
        - **Pre-Approved Communication Templates:** Pre-approved templates for recovery status updates, client notifications, and

final recovery reports are maintained to ensure consistency and clarity in communication.

- **Crisis Communication Drills:** Regular communication drills are conducted to ensure all stakeholders understand their roles and responsibilities and are prepared for actual recovery scenarios.

Roles and Responsibilities

- **Recovery Team:** Responsible for leading recovery efforts, coordinating with different departments, and ensuring all recovery steps are executed as planned.
- **IT Team:** Handles the technical recovery of systems, data restoration from backups, and verification of system integrity post-recovery.
- **Management Team:** Provides oversight and decision-making support during recovery, ensuring that recovery priorities align with business objectives.
- **Public Relations Team:** Manages external communication to clients, partners, and media to maintain transparency and trust.

Regular Review and Updates

This policy is reviewed annually and updated as needed to ensure it remains aligned with the organization's evolving needs and the cybersecurity threat landscape. Regular testing and simulations ensure that all teams remain prepared to execute recovery operations effectively.