Incident Response Policy

Purpose and Scope

This policy defines the procedures and actions to be taken by Mentornity to minimize the impact of a cybersecurity incident (e.g., data breach, malware attack) and protect the organization's reputation. This policy applies to all Mentornity employees, partners, and third-party vendors.

Policy Components

1. **Incident Response Plan (RS.RP - Response Planning)**
    - Mentornity has developed an Incident Response Plan (IRP) that outlines the steps to be taken in the event of a cybersecurity incident. This plan covers every phase from detection to recovery:
        - **Preparation:** An Incident Response Team (IRT) has been established, and response strategies for different types of incidents have been defined.
        - **Detection and Analysis:** SIEM systems and log monitoring tools are used to detect incidents at an early stage. Classification and analysis steps are planned for each type of incident.
        - **Containment and Eradication:** Actions such as isolating affected systems, removing malware, and recovering data are planned.
        - **Recovery:** A detailed recovery procedure is followed to safely return systems to normal operations.
        - **Post-Incident Review:** A comprehensive review is conducted after each incident, and lessons learned are recorded.
2. **Communication Strategy (RS.CO - Communications)**
    - Effective incident response requires clear communication with internal and external stakeholders:
        - **Internal Communication:** Rapid and clear communication is established with relevant teams such as IT, Legal, Public Relations, and Senior Management during and after an incident.

        - **External Communication:** Customers, partners, and regulatory bodies are informed following crisis communication protocols.
        - **Pre-Approved Communication Templates:** Ready-to-use notification and update templates are created based on the type and severity of the incident.
        - **Drills and Training:** Regular drills are conducted to test the effectiveness of communication plans.
3. **Continuous Improvement and Evaluation (RS.IM - Improvements)**
    - Continuous improvement of incident response processes involves the following steps:
        - **Post-Incident Review and Reporting:** After each incident, a comprehensive review is conducted to assess the effectiveness of the response process. The findings are shared with the management team, and potential improvements are identified.
        - **Applying Lessons Learned:** Incident response plans and protocols are updated based on the findings from review reports.
        - **Regular Drills and Tests:** Incident response plans are regularly tested and reinforced with drills.

Roles and Responsibilities

- **Incident Response Team (IRT):** Responsible for executing response strategies during an incident and coordinating with other teams.
- **IT Team:** Conducts the technical analysis of the incident, isolates affected systems, and manages the recovery process.
- **Legal and Compliance Team:** Ensures compliance with legal requirements and handles necessary legal notifications.
- **Public Relations Team:** Responsible for external communication and all crisis communication strategies related to the organization's reputation.

Regular Review and Updates

This policy is reviewed annually and updated as needed to align with the organization's evolving needs and threat landscape. Regular drills and training keep all teams prepared.