SIP Security Incident Plan Policy:

Introduction:

1. Purpose:
   This Security Incident Plan (SIP) outlines the procedures to be followed in the event of a security incident. The plan's goal is to minimize the impact of security incidents on the organization's assets, data, and reputation.

2. Scope and Applicability:
   This plan is applicable to all systems and assets owned or managed by the organization and all personnel who use them.

Definitions:

- Security Incident: Any event that may compromise the confidentiality, integrity, or availability of the organization's assets or data.
- Incident Response Team (IRT): A designated team of individuals responsible for responding to security incidents.
- Incident Severity Levels: A classification scheme used to prioritize security incidents based on their potential impact.

3. Roles and Responsibilities:

A. Incident Response Team (IRT) Leader: The IRT leader is responsible for coordinating the incident response effort, communicating with stakeholders, and ensuring that all necessary actions are taken.
B. Incident Response Team (IRT) Members: IRT members are responsible for executing the incident response plan and following the procedures outlined in the plan.
C. Other Roles and Responsibilities: Any other roles and responsibilities specific to the organization should be defined here, including contact information for each role.

4. Incident Response Process:

1. Detection: The process of identifying a security incident.
2. Analysis: The process of determining the scope and impact of a security incident.
3. Containment: The process of limiting the impact of a security incident.
4. Eradication: The process of removing the cause of a security incident.
5. Recovery: The process of restoring affected systems or assets to their normal state.
6. Communication: The process of communicating with stakeholders throughout the incident response process.

5. Incident Classification and Prioritization:
   A. Incident Severity Levels:

- Level 1: Low impact incidents that can be handled without significant disruption to business operations.
- Level 2: Medium impact incidents that may require some business operations to be suspended or modified.
- Level 3: High impact incidents that may cause significant disruption to business operations.

B. Prioritization Framework: Incidents will be prioritized based on their severity level and the potential impact on the organization.

6. Incident Handling Procedures:

- Containment: The organization will isolate affected systems or assets to prevent the spread of the incident.
- Evidence Preservation: The organization will preserve any evidence related to the incident in a forensically sound manner.
- System Recovery: The organization will restore affected systems or assets to their normal state.

7. Reporting and Documentation:

- Incident Reporting: All incidents will be reported to the IRT leader as soon as they are detected.
- Documentation: The organization will document all incidents, including the incident type, severity level, and any actions taken.

g. Training and Awareness:

- Training Programs: The organization will provide training to all personnel on the incident response process and their roles and responsibilities in the process.
- Awareness Campaigns: The organization will conduct awareness campaigns to promote the importance of incident response and encourage reporting of incidents.

h. Testing and Improvement:

- Incident Response Exercises: The organization will conduct periodic incident response exercises to test the effectiveness of the incident response plan and identify areas for improvement.
- Analysis and Improvement: The organization will analyze all incidents and their response to identify areas for improvement in the incident response plan.

Authored by Geneva Knott
Document Version: 1.0 Last Updated: May 12, 2023
Next Review: May 12, 2024