Incident Response Policy

# 1. Purpose:

This Incident Response Policy aims to provide a framework for identifying, responding to, and mitigating security incidents within our MSSP SOC. This policy applies to all SOC personnel involved in incident response activities.

# 2. Scope:

This policy covers incident response for a diverse clientele, including LokDon, AINautics, Cyberlockx, and medium-sized businesses. It encompasses the entire incident response process, from detection and classification to resolution and recovery.

# 3. Incident Response Model:

The SOC employs the NIST SP 800-61 Incident Handling Process as a foundation for incident response. This model consists of the following phases:

a. Preparation: The SOC maintains an incident response capability, including continuous staff training, documentation, and suitable tools.

b. Detection and Analysis: Continuous monitoring of client systems is performed around the clock to identify potential security incidents, leveraging a range of tools and techniques.

c. Containment, Eradication, and Recovery: Upon confirmation of an incident, the SOC acts swiftly to contain the situation, eliminate the threat, and work on restoring normal operations.

d. Post-Incident Activity: Following incident resolution, a thorough post-incident review is conducted to glean insights, identify areas for improvement, and enhance security measures.

# 4. Incident Priority and Classification Criteria:

The effective management of incidents relies on the following criteria:

a. Severity Levels: Incidents are classified into different severity levels: Critical, High, Medium, or Low, based on their potential harm and impact on clients' operations.

b. Client Impact: The impact on clients' operations, data, and reputation is evaluated, with higher priority assigned to incidents affecting critical systems or data.

c. Regulatory and Legal Considerations: Incidents are assessed in accordance with the legal and regulatory requirements specific to each client's industry.

d. Relevance to Business Operations: The continuity of business operations is considered, including access to essential resources and services.

e. Public Relations and Reputation: The potential impact on the client's reputation and the MSSP is assessed.

# 5. Incident Response Procedure:

Detailed incident response procedures are documented for each phase of the NIST SP 800-61 model:

NIST Special Publication 800-61 Revision 2, titled "Computer Security Incident Handling Guide." You can find it on the official NIST website. - [1]

a. Incident Detection and Analysis: Techniques for detecting and assessing potential incidents, using various monitoring tools and methodologies.

b. Incident Containment and Eradication: Procedures for containing incidents, identifying root causes, and eliminating threats, with a focus on minimizing client impact.

c. Recovery and Post-Incident Activities: Steps for restoring normal operations, conducting post-incident reviews, and documenting lessons learned.

d. Communication and Notification: Guidelines for communicating with affected clients, legal authorities, and stakeholders, with a clear timeline for notification.

# 6. Training and Awareness:

Regular training for SOC personnel ensures their readiness to handle incidents effectively. Clients are educated on their roles and responsibilities within the incident response process.

# 7. Continuous Improvement:

The SOC regularly reviews and updates incident response procedures based on lessons learned and emerging threats. Improvements are documented and implemented promptly.

# 8. Client-Specific Procedures:

Acknowledging the uniqueness of each client's requirements, the SOC maintains client-specific incident response procedures, ensuring alignment with their specific needs, objectives, and regulations.

This policy provides a clear and precise framework for our SOC to respond effectively to security incidents within the context of 24/7/365 continuous incident response. We understand that each incident is unique, and response times will be reasonable based on the specific circumstances, while still adhering to our commitment to security and client support. Collaboration with each client is vital to ensure their individual requirements are met.

# Appendix

[1] [NIST SP 800-61 Revision 2 - Computer Security Incident Handling Guide](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)