**Cybersecurity Respond Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity respond policy is to establish guidelines and procedures for responding to cybersecurity incidents promptly, effectively, and efficiently, in alignment with the NIST Cybersecurity Framework (CSF) Version 2.0.

1.2. Scope: This policy applies to all employees, contractors, and third-party vendors who have access to the organization's information systems and networks.

**2. Incident Response Team**

2.1. Formation:

* An incident response team shall be established comprising individuals with specialized skills in incident detection, analysis, containment, eradication, and recovery.
* The incident response team shall include representatives from relevant departments including IT, HR, and legal, and communications.

2.2. Roles and Responsibilities:

* Incident response team members shall have clearly defined roles and responsibilities, including incident coordinator, technical analysts, legal advisors, and communications liaisons.
* Responsibilities shall include coordinating response efforts, conducting forensic analysis, notifying stakeholders, and managing communication with internal and external parties.

**3. Incident Handling Procedures**

3.1. Incident Classification:

* Incidents shall be classified based on severity, impact, and potential risk to the organization's operations, assets, and reputation.
* Incident classification criteria shall be predefined and documented to facilitate consistent and timely response.
* Incidents will be escalated where necessary if the severity and impact are above a pre-defined risk

3.2. Response Plan Activation:

* Upon detection of a cybersecurity incident, the incident response plan shall be activated immediately.
* The incident response coordinator shall be responsible for initiating the response plan and coordinating response activities.

**4. Incident Containment and Mitigation**

4.1. Containment Measures:

* Immediate containment measures shall be implemented to prevent further spread or escalation of the incident.
* Isolation of affected systems, disabling compromised accounts, and blocking malicious network traffic shall be prioritized to contain the incident.

4.2. Mitigation Strategies:

* Mitigation strategies shall be developed and implemented to remediate the effects of the incident and restore affected systems and services to normal operation.
* Remediation activities shall be conducted in accordance with predefined response procedures and best practices.

**5. Forensic Analysis**

5.1. Evidence Preservation:

* Forensic evidence shall be preserved to support investigation and analysis of the incident.
* Chain of custody procedures shall be followed to maintain the integrity and admissibility of digital evidence.

5.2. Root Cause Analysis:

* Root cause analysis shall be conducted to determine the underlying cause of the incident and identify vulnerabilities or weaknesses in the organization's security posture.
* Findings from root cause analysis shall be used to implement corrective actions and prevent similar incidents in the future.

**6. Communication and Notification**

6.1. Stakeholder Notification:

* Communication with internal and external stakeholders shall be managed effectively to provide timely updates on the incident response efforts.
* Notification procedures shall be established to inform affected parties, regulatory authorities, and law enforcement agencies as required by applicable laws and regulations.

6.2. Media and Public Relations:

* Communications with the media and public shall be coordinated through designated spokespersons to ensure accurate and consistent messaging.
* Media response plans and templates shall be prepared in advance to streamline communication during crisis situations.

**7. Recovery and Resumption**

7.1. System Recovery:

* Recovery efforts shall be prioritized based on the criticality and importance of affected systems and services.
* Backup and restoration procedures shall be followed to recover data and restore functionality to pre-incident state.

7.2. Business Continuity:

* Business continuity plans shall be activated to minimize the impact of the incident on organizational operations and ensure continuity of essential functions.
* Alternate processing capabilities and contingency measures shall be implemented to maintain business continuity during the incident response and recovery process.

**8. Lessons Learned and Improvement**

8.1. Post-Incident Review:

* After the incident has been resolved, a post-incident review shall be conducted to evaluate the effectiveness of the response efforts and identify lessons learned.
* Findings from the post-incident review shall be used to update incident response procedures, enhance security controls, and improve overall incident response readiness.

**9. Review and Revision**

9.1. Policy Review:

* This cybersecurity respond policy shall be reviewed and updated periodically to reflect changes in the organization's technology environment, business operations, and regulatory requirements.
* Reviews shall be conducted at least annually or more frequently as needed.

**Reference Documents**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |