**Cybersecurity Recover Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity recover policy is to establish guidelines and procedures for recovering from cybersecurity incidents and disruptions, restoring affected systems and data, and resuming normal operations 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 Continuity**

2.1. Continuity Planning:

* Business continuity and disaster recovery plans shall be developed and maintained to ensure the organization's ability to respond to and recover from cybersecurity incidents and disruptions.
* Continuity plans shall address key aspects such as data backup and restoration, system recovery, alternate processing capabilities, and personnel roles and responsibilities.

2.2. Incident Response Coordination:

* The incident response team shall coordinate closely with business continuity and disaster recovery teams to ensure a seamless transition from incident response to recovery and resumption of normal operations.
* Recovery priorities and strategies shall be aligned with business objectives and critical functions to minimize the impact of disruptions on organizational operations.

**3. Data Backup and Restoration**

3.1. Backup Procedures:

* Regular backups of critical data and information systems shall be performed in accordance with predefined backup schedules and retention policies.
* Backup procedures shall include verification of backup integrity, encryption of backup data, and secure storage in offsite or cloud-based repositories.

3.2. Restoration Processes:

* Procedures for restoring data from backups shall be documented and tested periodically to ensure timely recovery in the event of data loss or corruption.
* Restoration efforts shall prioritize critical data and systems essential for maintaining business operations and continuity.

**4. System Recovery and Resumption**

4.1. Recovery Time Objectives (RTOs):

* Recovery time objectives (RTOs) shall be established for different types of systems and services based on their criticality and importance to the organization's operations.
* RTOs shall define the maximum acceptable downtime for each system or service before recovery and resumption efforts must be completed.

4.2. Recovery Strategies:

* Recovery strategies shall be developed and implemented to restore affected systems and services to operational status within the defined RTOs.
* Strategies may include system rebuilds, data restoration, failover to alternate processing sites, and cloud-based recovery solutions.

**5. Incident Communication and Reporting**

5.1. Stakeholder Notification:

* Communication with internal and external stakeholders shall be maintained throughout the recovery process to provide updates on recovery efforts and expected timelines.
* Stakeholders shall be informed of progress, challenges, and any changes to recovery plans or priorities.

5.2. Post-Incident Reporting:

* After recovery efforts have been completed, a post-incident report shall be prepared to document the incident response and recovery activities, including lessons learned, challenges encountered, and improvements made.
* The post-incident report shall be shared with relevant stakeholders and used to enhance future incident response and recovery capabilities.

**6. Lessons Learned and Improvement**

6.1. Post-Incident Review:

* A post-incident review shall be conducted to evaluate the effectiveness of recovery efforts and identify opportunities for improvement.
* Findings from the post-incident review shall be used to update recovery procedures, enhance resilience measures, and improve overall incident response and recovery readiness.

6.2. Continuous improvement

* Exercises and tests will be executed at least bi-annually.
* Exercise and test results will help confirm or refute assumptions that were made in planning,

particularly regarding how realistic the recovery targets are.

**7. Review and Revision**

7.1. Policy Review:

* This cybersecurity recover 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**

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