**Cybersecurity Protect Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity protect policy is to establish guidelines and procedures for implementing safeguards and controls to protect information assets, systems, and data from cybersecurity threats and vulnerabilities, 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 data assets.

**2. Access Control**

2.1. User Access:

* Access to information systems and data shall be granted based on the principle of least privilege, ensuring that users have only the minimum level of access necessary to perform their job functions.
* User access shall be authenticated and authorized through secure mechanisms such as strong passwords, multi-factor authentication, and role-based access controls.

2.2. Privileged Access:

* Privileged access to critical systems and data shall be restricted to authorized personnel only.
* Privileged accounts shall be monitored and audited regularly to prevent unauthorized access and detect suspicious activities.

**3. Data Security**

3.1. Encryption:

* Data shall be encrypted both in transit and at rest to protect it from unauthorized access and interception.
* Strong encryption algorithms and key management practices shall be used to ensure the confidentiality and integrity of sensitive information.

3.2. Data Loss Prevention:

* Data loss prevention (DLP) mechanisms shall be implemented to prevent the unauthorized disclosure or leakage of sensitive information.
* DLP controls shall monitor and block the transmission of sensitive data through email, web, and other communication channels.

**4. Security Awareness and Training**

4.1. Employee Training:

* All employees shall receive regular training on cybersecurity best practices, including phishing awareness, password security, and safe browsing habits.
* Training programs shall be tailored to employees' roles and responsibilities and conducted at least annually.

4.2. Incident Response Training:

* Incident response teams shall receive specialized training on responding to cybersecurity incidents, including incident detection, containment, eradication, and recovery procedures.
* Tabletop exercises and drills shall be conducted periodically to test the effectiveness of incident response plans.

**5. Security Configuration Management**

5.1. Secure Configuration:

* Information systems and devices shall be configured securely according to industry best practices and vendor recommendations.
* Configuration baselines shall be established and regularly updated to mitigate known vulnerabilities and weaknesses.

5.2. Patch Management:

* Patch management procedures shall be implemented to ensure that security patches and updates are applied promptly to mitigate newly discovered vulnerabilities.
* Critical patches shall be prioritized and deployed in a timely manner to reduce the risk of exploitation.

**6. Third-Party Risk Management**

6.1. Vendor Security Assessment:

* Third-party vendors and service providers shall undergo security assessments to evaluate their cybersecurity practices and controls.
* Contracts and agreements with third-party vendors shall include provisions for security requirements, data protection, and incident response obligations.
* All new and existing software will undergo an initial security check before installation and be reviewed, if necessary, removed.

**7. Incident Response**

7.1. Incident Reporting:

* Employees shall be trained to report cybersecurity incidents promptly to the designated incident response team.
* Incident reporting procedures shall include guidelines for documenting incident details, preserving evidence, and notifying appropriate stakeholders.

7.2. Incident Response Plan:

* An incident response plan shall be developed and maintained to guide the organization's response to cybersecurity incidents.
* The incident response plan shall define roles and responsibilities, communication procedures, and escalation paths for different types of incidents.

**8. Continuous Monitoring**

8.1. Threat Monitoring:

* Continuous monitoring of information systems and networks shall be conducted to detect and respond to cybersecurity threats in real-time.
* Threat intelligence sources shall be monitored to identify emerging threats and vulnerabilities relevant to the organization's operations.

**9. Review and Revision**

9.1. Policy Review:

* This cybersecurity protect 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**

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