**Cybersecurity Governance Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity governance policy is to establish a framework for effectively managing and improving our organization's cybersecurity posture 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. Governance Structure**

2.1. Cybersecurity Steering Committee: A cybersecurity steering committee will be established consisting of senior management representatives from relevant departments, including but not limited to IT, legal, compliance, and risk management.

2.2. Roles and Responsibilities:

* The cybersecurity steering committee is responsible for overseeing the implementation, monitoring, and continuous improvement of cybersecurity practices within the organization.
* The Group Head of IT (tbc) will serve as the chairperson of the cybersecurity steering committee and will be responsible for coordinating cybersecurity efforts across all departments.
* The committee will be responsible for overseeing the relevant legal requirements are met e.g. GDPR, Australian privacy act etc
* Individual departments and business units are responsible for implementing and adhering to cybersecurity policies and procedures in their respective areas.

**3. Risk Management**

3.1. Risk Assessment:

* Regular risk assessments will be conducted to identify and prioritize cybersecurity risks to the organization's information systems and data assets.
* Risk assessments will be performed using the methodology outlined in the NIST, taking into account threats, vulnerabilities, and potential impacts.

3.2. Risk Mitigation:

* Based on the results of risk assessments, appropriate controls and safeguards will be implemented to mitigate identified risks to an acceptable level.
* Controls will be selected based on industry best practices and the guidance provided by the NIST.

**4. Security Controls**

4.1. Security Control Framework:

* A comprehensive set of security controls will be established based on the NIST and other relevant cybersecurity frameworks, standards, and regulations.
* Security controls will be tailored to the organization's specific business needs and risk profile.

4.2. Control Implementation:

* IT and security teams will be responsible for implementing and maintaining the necessary technical, administrative, and physical security controls to protect the organization's information systems and data assets.

**5. Continuous Improvement**

5.1. Monitoring and Evaluation:

* Continuous monitoring of cybersecurity controls and processes will be conducted to ensure effectiveness and compliance with established policies and standards.
* Regular evaluations and reviews will be performed to identify areas for improvement and address emerging threats and vulnerabilities.

5.2. Incident Response and Management:

* An incident response plan will be developed and maintained to effectively respond to and mitigate cybersecurity incidents.
* Incident response procedures will be tested through regular tabletop exercises and drills to ensure readiness.
* A library of playbooks will be readily available to deal with the most common issues and those that have affected us, these will be updated and maintained to ensure the best industry standards.

**6. Compliance and Enforcement**

6.1. Compliance:

* All employees, contractors, and third-party vendors are required to comply with this cybersecurity governance policy and associated procedures.
* Non-compliance may result in disciplinary action, up to and including termination of employment or contract.

6.2. Enforcement:

* The cybersecurity steering committee (TBD), in conjunction with HR and legal departments, will be responsible for enforcing this policy and addressing instances of non-compliance.

**7. Review and Revision**

7.1. Policy Review:

* This cybersecurity governance policy will be reviewed and updated on an annual basis or as necessary to reflect changes in the organization's risk profile, business operations, or regulatory requirements.

7.2. Stakeholder Engagement:

* Stakeholders from relevant departments will be involved in the review and revision process to ensure alignment with business objectives and priorities.

**8. Document Control**

8.1. Policy Distribution:

* This cybersecurity governance policy will be distributed to all employees, contractors, and third-party vendors with access to the organization's information systems and data assets.

8.2. Policy Documentation:

* A record of policy distribution and acknowledgement will be maintained, and employees will be required to acknowledge receipt and understanding of the policy.

**Reference Documents**

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