MARINUS LINK

Information Security Policy

Purpose

This policy outlines the ways we can help prevent or minimise the impact of information security incidents or breaches at MLPL and protect MLPL's business and reputation.

Applying our policy principles will help us safeguard our people, customers, and stakeholders.

We align with 'ISO 27001:2022 Information security, cybersecurity and privacy protection' and 'ACSC's Essential 8' that together:

- provide a framework for managing the security of MLPL's information systems and assets
- assist MLPL to ensure the confidentiality, integrity, and availability of our information systems and assets
- identify the roles, responsibilities, and accountability of users as it relates to information security
- provide guidance for ensuring mature controls are adopted.

This policy is to be read together with our:

- Privacy Policy
- Information Management Policy
- Acceptable Use Policy
- Reporting a Non-Compliance Procedure.

Scope

This policy applies to the MLPL Board, our employees, contractors and service providers with access to MLPL's information assets and resources.

Our Policy Principles

We apply the following policy principles to ensure the security of MLPL's information assets:

Risk management – we will identify and manage cyber security risk to our systems, assets, data, and capabilities.

Appropriate controls – we will implement appropriate cyber security controls to protect the delivery of critical infrastructure services.

Authorised users – MLPL's information, communication and technology services and facilities are for use by authorised users only and governed by appropriate controls.

Incident management – MLPL will maintain frameworks, plans and systems to identify the occurrence of cyber security events and will respond to events and restore the capabilities or services.

Accountability – users of the MLPL information, communication and technology services and facilities will understand their cyber security obligations and report all cyber security incidents and events.

Access control – MLPL may, where appropriate, monitor and restrict the use of the company's services and facilities.

Personally owned devices – Access to MLPL's systems from personally owned devices is subject to the security requirements of this policy.

Life cycle management – systems and applications will be designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.

Ongoing monitoring – we will conduct internal audits to assess and inform whether the information security capabilities of MLPL align with the business' requirements and are being effectively implemented and maintained.

Continuous improvement – we will continually improve the suitability, adequacy, and effectiveness of MLPL's security controls, policies and practices.

Patch management – we will ensure that information processing systems are regularly patched and maintained according to supplier recommendations and industry practices.

Business continuity – we will ensure that critical systems are regularly and securely backed up to ensure that data availability and integrity is maintained in the event of an error, compromise, failure or disaster.

Leadership - information security is governed within MLPL by the Senior Leadership Team who sponsor:

- the information security strategy
- the planning, monitoring, reviewing and ensuring the effectiveness of the overall information security framework, which is part of the MLPL's Policy Framework
- the development of industry standard and business aligned information security practices and processes
- measuring the effectiveness of the information security program through the collection and analysis of metrics, self-assessments and independent review.

Caroline Wykamp 21 March 2024
Chief Executive Officer
Marinus Link