kiland

Kiland Cyber Security Policy

Intent

This policy:

- Provides the foundation for Cybersecurity management within **Kiland**;
- Supports the achievement of **Kiland** outcomes; and
- Supports **Kiland's** commitment to meet its statutory, legal, and moral obligations by administering its information holdings in a lawful and ethical manner.

Scope

This Policy applies to:

- **Kiland's** Information and Communication Technology (ICT) Services;
- All Authorised Users of **Kiland's** ICT managed by the **Kiland** or third party providers on behalf of the **Kiland**; and
- **Kiland's** tangible and intangible assets including:
  - **Kiland's** reputation and public image; and
  - **Kiland's** information in any medium or form such as electronic (digital, video or audio representations) or printed paper.

This Policy does not apply to **Kiland's** Controlled Entities.

Definitions

Acceptable Use – means those behaviours and actions, in connection with the use of **Kiland's** ICT Services, which are permitted under the ICT Acceptable Use Policy.

Accountable Officer – means the senior staff member with accountability for Cybersecurity within **Kiland's**.

Asset Owner – means an individual or collective group with accountability and authority for **Kiland's** ICT Services.

Authorised User – means a person who has been provided with an Authentication Credential by **Kiland** to access **Kiland's** ICT Services.

Authentication Credential – means a userID/password, username/passcode, PIN or other secret keys used to gain access to ICT Services.

Capability – the capacity, materials and expertise an organisation needs in order to perform a business function.

Control – means a measure put in place to eliminate or minimise risk.

Cybersecurity – means the methods (policies, strategies, behaviours and techniques) through which necessary and commensurate measures can be identified, implemented, and maintained to effect Information Security.

Information Security – means the protection and preservation of the confidentiality, integrity and availability of information in digital or other means.

Reasonably Practicable – means that which is, or was at a particular time, reasonably able to be done to ensure Information Security, taking into account and weighing up all relevant matters including:

- the likelihood of risk concerned occurring;
- the consequence that might result from the threat or the risk;
- what the person concerned knows, or ought reasonably to know, about the risk, and about the ways of eliminating or minimising the risk;
- the availability and Suitability of Controls to eliminate or minimise the risk; and
- after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

Responsible Officer – means a senior staff member or committee who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business, namely a Director, CEO, CFO, CIO.

Suitability of Control – means the suitability of a particular Control having regard to whether or not the Control:

- is effective in eliminating or minimising risk or the likelihood of risk
- does not introduce new and higher risks in the circumstances; and
- is practical to implement in the circumstances in which risk exists

Kiland's ICT Services – means facilities and services provided to an Authorised User including software, communication devices, and computing infrastructure under the control of **Kiland** (or a third-party provider on **Kiland's** behalf) that provides access to information in online or electronic format.

Introduction

Effective protection of business information creates a competitive advantage, both in the ability to preserve the reputation of **Kiland's** brand and in reducing the risk of the occurrence of negative events and incidents.

Our aim is to be more resilient to cyber-attacks and better able to protect our interests in the digital economy.

Effective Cybersecurity requires an enterprise approach to ensure each responsible entity has the procedures, tools and support required to undertake its business effectively while managing the risk of adverse security incidents and events.

This policy does not assure protection against all security threats or attacks that may interrupt core services of **Kiland**. Instead, this Policy supports **Kiland** in demonstrating that Cybersecurity risks and measures are being identified and managed in a way that is appropriate for the information value, business environment, and objectives of **Kiland**, namely:

- The sponsorship of a Cybersecurity Capability;
- The institution of accountability and responsibilities with respect to Cybersecurity;
- Promotion of an intentional Information Security culture;
- The establishment of an Information Security risk management program including criteria through which security risks will be evaluated and accepted; and
- Establishing methods for the response to Information Security threats and incidents.

Policy principles

1. Capability

Kiland management will:

- Sponsor a Cybersecurity Capability to identify, analyse, and mitigate Information Security risk to the organisation, including its business units, subsidiaries, related interconnected infrastructure, stakeholders and suppliers in accordance with this Policy.
- Nominate an Accountable Officer.

The Accountable Officer will:

- Establish **Kiland's** Cybersecurity Capability based on the following principles:
- Positive reinforcement of Information Security responsibilities.
- Proactive assessment, evaluation and management of Information Security risk(s).
- Proactive monitoring and response to Information Security threats and incidents.

2. Responsibilities

The Accountable Officer will:

- Establish **Kiland's** Cybersecurity Management Plan that aligns to the core requirements of the Queensland Government's information security policies and standards.
- Establish Cybersecurity roles and responsibilities and document these responsibilities in the **Kiland's** Cybersecurity Management Plan.
- Establish measurable objectives, targets and outcomes to drive continual improvement aimed at reducing Information Security risks, events and incidents.
- Assure the effectiveness of the Cybersecurity Capability, as required.

The Responsible Officers will:

- Support the Cybersecurity Capability through the establishment and implementation of relevant processes, procedures, standards, and guidelines as outlined in **Kiland's** Cybersecurity Management Plan.

3. Culture

The Responsible Officers will:

- Promote and sustain an intentional Information Security culture throughout **Kiland's** , ensuring all Authorised Users:
- develop a sense of ownership in the protection of all information; and
- hold themselves accountable for their actions, (including the Acceptable Use of **Kiland's** ICT Services).
- Support role specific awareness, training and education to Authorised Users.
- Promote the reporting of Information Security events and incidents, including recognition for those Authorised Users who act in support of Information Security.
- Ensure Information Security is considered as a requirement in all new projects and initiatives, regardless of the type of project.
- Proactively collaborate and support stakeholders (including audit) on Information Security matters.

4. Risk Management

The Accountable Officer will:

- Establish and operate an information-centric risk management program that provides a systematic approach to the identification, analysis and evaluation of Information Security risk including business units, related interconnected infrastructure, subsidiaries, stakeholders and suppliers.
- Facilitate informed risk acceptance by ensuring recognised risks are appropriately documented and passed to the appropriate Responsible Officer, in line with **Kiland's** Risk Management Policy and Framework and accompanying risk appetite statement.

- Establish the **Kiland's** Cybersecurity Management Plan that:
  - Establishes the Cybersecurity goals; and
  - Details the baseline Information Security Controls for **Kiland's** in the management of Information Security risks.
- Report on Information Security risks and achievement of goals on a routine basis.

The Responsible Officers and Asset Owners will:

- Implement relevant Controls from the **Kiland's** Cybersecurity Management Plan.
- Treat identified risks through the implementation of Reasonably Practicable Controls to protect **Kiland's** information and related information systems against loss of confidentiality, integrity or availability.
- Monitor, assess and continually improve the Suitability of Controls on a periodic basis.

5. Response and Recovery

The Accountable Officer will:

- Establish, implement and rehearse a Cybersecurity Incident Response Plan to prepare for, respond to, and recover from disruptive cyber-incidents.

The Responsible Officers and Asset Owners will:

- Provide reasonable resources to support the implementation and operation of the Cybersecurity Incident Response Plan.