

IT4 - IT SECURITY POLICY

Purpose

IT resources play a crucial role in the development and sharing of information and in supporting the advancement of knowledge at **Freightways**. The purpose of this policy is to define responsibilities within each unit for maintaining the security of the IT resources under their control.

By implementing this policy **Freightways** will:

- protect against unauthorised access to, or unauthorised use or sharing of data that could potentially result in harm to **Freightways** or to members of **Freightways group**
- protect against anticipated threats or hazards to the security of IT resources
- comply with legal requirements, **Freightways** policies and any agreements binding **Freightways** to implement applicable security safeguards

Policy Application

This policy applies to all members of the **Freightways group** whether at a **Freightways site** or elsewhere and refers to all IT resources.

Definitions

Term	Definition
Critical data	Refers to the importance of the data to the operation of Freightways.
Freightways	Freightways Limited and its subsidiary companies together or individually as the context implies.
Freightways Group	includes all staff members (whether permanent, temporary or part time), contractors, subcontractors, consultants, business partners or official visitors or guests of members of Freightways staff.
Heads of unit	General Managers, Freightways CEO, Freightways CFO, Freightways CIO.
Information Security	The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data.
IT security incident	Includes an attempted or successful unauthorised access, use, disclosure, modification or destruction of information, or interference with IT operation
IT resources	refers to any Freightways owned or operated hardware or software and the data that is used or stored on it.

IT user	means any individual member of the Freightways group using IT resources.
Personal Information	Information about an identifiable individual
Sensitive data	Refers to data whose unauthorised disclosure may have serious adverse effect on individuals or on Freightways reputation, resources, or services
Security safeguards	Measures undertaken to protect IT resources.
Unit	refers to an organisational grouping across Freightways and includes Business Units, Internal Service providers.

Key Relevant Documents

Include the following:

- Freightways – IT Acceptable Use Policy
- Freightways – Offensive Materials Policy
- Freightways – IT Institutional Data Management Policy
- Freightways – IT Privacy and Monitoring Policy
- Freightways – Electronic Communications Policy
- Freightways – IT Password Policy
- [Privacy Act 2020](#) (NZ)
- [Privacy Act 1998](#) (AU)

Roles and Responsibilities

Freightways group staff must maintain awareness and adherence to applicable IT policies, standards and guidelines.

The Executive Management of Freightways is responsible for:

- Reviewing and approving all IT related policies.

Heads of unit are responsible for:

- Communicating and applying IT policies, standards and guidelines within their unit.
- Assigning individuals to unit information security roles, ensuring they are properly trained and ensuring their on-going participation in **Freightways group** security activities.
- Ensuring the implementation of information security plans within their unit
- Ensuring unit collaboration on the implementation of **Freightways group** IT security programmes.

The Chief Information Officer of Freightways is responsible for:

- Directing and coordinating the **Freightways group** IT Security Programme including the creation and maintenance of IT related policies, standards and guidelines.
- Determining unit level compliance with IT policy, standards and guidelines

- Providing a focal point for oversight of serious security incidents
- Establishing security metrics, tracking the progress of the IT Security Programme and providing a **Freightways group** IT risk profile
- Ensuring availability of appropriate information, education and training

Policy

1. **IT users** at **Freightways** have individual and shared responsibilities to ensure the protection of **IT resources**.
2. Each **unit** will develop, maintain, and implement an information security plan.
3. The plan will identify applicable regulations and will define unit security safeguards.
4. Each **unit** will identify and track sensitive and **critical data** under its control.
5. Each **unit** will identify, track and protect **personal information** under its control in accordance with the Privacy Act applicable to the **unit's** jurisdiction.
6. Each **unit** will periodically conduct risk assessments around its sensitive and critical data.
7. Risk assessments will prioritise risks and recommend appropriate mitigation strategies.
8. Each **unit** will report and manage IT security incidents and/or privacy breaches in accordance with the security incident reporting procedures and the provisions of the Privacy Act applicable to the **unit's** jurisdiction.

Other IT-related policies

This IT Security Policy should be read in conjunction with all other Freightways IT-related policies.