Freightways

IT5 - IT INSTITUTIONAL DATA MANAGEMENT POLICY

Freightways

Purpose

Institutional data is a key asset of the **Freightways**. Successful management and protection of the **institutional data** under the care of the **Freightways** is critical to the business and administrative functions of the **Freightways group**.

This policy outlines responsibilities for the care of institutional data and serves to:

- ensure the establishment, maintenance, and delivery of secure, confidential, trustworthy, stable, reliable, and accessible collections of institutional data for shared access by the **Freightways group**
- maximise the value received from the data asset by increasing the understanding and use of the data

Policy Application

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

Definitions

Term	Definition
BYO	Bring Your Own
Critical data	Refers to the importance of the data to the operation of Freightways.
Freightways	Means Freightways Limited and includes all subsidiaries
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.
Institutional data	Includes a data element which satisfies one or more of the following criteria, it is: Relevant to planning, managing, operating, controlling, internal or external accountability or auditing of Freightways created, received, maintained, or transmitted as a result of business activities generally referenced or required for use by more than one organisational unit. Included in an official Freightways report. Data that Freightways is legally/ contractually obliged to hold Generated by an IT user using any of the above 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
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 Security Policy
- Freightways – IT Acceptable Use Policy
- Freightways – Software Use Policy
- Freightways – Electronic Communications Policy
- Privacy Act 2020 (NZ)
- Privacy Act 1988 (AU)
- Copyright Act 1994 (NZ)
- Copyright Act 1968 (AU)

Roles and Responsibilities

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

Heads of units are responsible for communicating and applying IT policies, standards and guidelines within their unit.

Freightways

Policy

1. **IT Users** must take all reasonable care to protect institutional data from unlawful or unauthorised access, alteration or destruction and/or inappropriate disclosure or use

2. Access to institutional data will be granted only with appropriate and lawful authorisation, based on the proposed user's role and the intended use of the data

3. Authorisation and access to **critical** and sensitive **data** will be documented, reviewed, modified, and terminated as appropriate

4. Each **unit** will develop and implement data classification schema and guidelines.

5. Each **unit** will develop and implement data management plans that address the quality, availability and accessibility of the data throughout its lifecycle

6. Each **unit** will ensure there data management plans address specifically the quality, availability and accessibility of data with regard to mobile or BYO devices.

7. Contingency plans will be developed and implemented. Disaster Recovery/Business Continuity plans and other methods of responding to an emergency or other occurrence of damage to systems containing institutional data will be developed, implemented, and maintained

Other IT-related policies

This IT Institutional Data Management Policy should be read in conjunction with all other Freightways IT-related polices.