Freightways

# IT6 - ELECTRONIC COMMUNICATIONS POLICY

Freightways

## Purpose

The **Freightways** considers the appropriate use of Electronic Communications (including E-mail & the Internet) as important in achieving business goals.

The objectives of this policy are:

- To provide guidance to employees on how they can appropriately utilise the **Freightways** electronic communications systems;
- To ensure that the **Freightways** electronic communication systems are used for the positive conduct of the **Freightways** business activities;
- To uphold the reputation of the **Freightways** in its dealings with employees, contractors, clients and members of the public.
- To prevent the exfiltration of the **Freightways institutional data**.

## 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 |
|---|---|
| **DLP** | Means data loss prevention, means to prevent the exfiltration of data from the business through unauthorised means. |
| **FIS** | Freightways Information Services Ltd. |
| **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 |
| **Institutional data** | Includes a data element which satisfies one or more of the following criteria.<br>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.<br>Included in an official Freightways report.<br>Data that Freightways is legally/ contractually obliged to hold. Generated by an IT user using any of the above data. |

| | |
|---|---|
| **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. |
| **Unit(s)** | 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 - Offensive Materials Policy
- Freightways - IT Institutional Data Management Policy
- Freightways - IT Privacy and Monitoring Policy
- Unsolicited Electronic Messages Act 2007 (NZ)
- Spam Act 2003 (AU)

# Roles and Responsibilities

## Employees and Contractors

- Ensure they use the electronic communication systems in a manner that always contributes positively to the achievement of the **Freightways** business objectives.

## Management

- Explain the policy to employees as required and provide answers to any questions raised regarding the policy;
- Ensure that electronic communication systems are used responsibly for the conduct of **Freightways** business operations;
- Ensure that electronic communication systems are not used to send or solicit messages that may be considered to be offensive or disruptive to business operations; and
- Ensure that any complaints regarding possible breaches of this policy are reported and investigated promptly.

## FIS

- Audit **Freightways** systems to check that the electronic communications systems are being used appropriately; and
- Confidentially report to **Freightways** management any abuse of the electronic communications systems.

## Policy

1. In accordance with **Freightways** IT Acceptable use policy no electronic communication system is to be used for any unlawful or unethical purpose that may do harm to **Freightways**, employee's, contractors or any other persons.

2. All electronic communications to be appropriately classified and transmitted in line with **Freightways** or individual **unit** data classification schema and guidelines. This will include where appropriate the use of encryption to protect such communications during both transmission and storage.

3. In accordance with data classification and acceptable use requirements the use of data loss prevention (**DLP**) technologies will be employed to prohibit or quarantine communications to unauthorised third parties.

4. All automatically forwarded outbound emails to be appropriately authorised by **head of unit** or authorised delegate and advise **FIS** Security team in order to protect unauthorised exfiltration of **Freightways** or **Freightways** client information.

    a. **FIS** Security Team will be automatically notified of the creation of any such rules and follow up on all unauthorised rule creations.

    b. In line with policy item three **DLP** may be used to prohibit the transmission of unauthorised automated outbound communications.

## Other IT- related policies

This Electronic Communications Policy should be read in conjunction with all other Freightways IT- related polices.