Freightways

IT2 - SOFTWARE USE POLICY

Freightways

Purpose

The purpose of this policy is to provide guidelines for the appropriate use of software on company computer hardware.

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
FIS	Freightways Information Services Limited
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 unauthorised 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.
ISO27001	Is an information security standard, part of the ISO/IEC 27000 family of standards. ISO/IEC 27001:2013 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

SOC2 Type II	SOC stands for "system and organization controls," and the controls are a series of standards designed to help measure how well a given service organization conducts and regulates its information. SOC 2 is designed for service providers storing customer data in the cloud. It requires companies to establish and follow strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.
Software	Includes all computer programs in machine readable and printed form, together with associated manuals and other related documentation.
SaaS	Software as a Service
SOE	Standard Operating Environment
Unit(s)	Refers to an organisational grouping across **Freightways** and includes Business Units, Internal Service providers.

Key Relevant Documents

Include the following:

- Privacy Act 2020 (NZ)
- Privacy Act 1988 (AU)
- Copyright Act 1994 (NZ)
- Copyright Act 1968 (AU)
- Freightways - IT Security Policy
- Freightways - IT Privacy and Monitoring Policy

Roles and Responsibilities

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

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

FIS is responsible for auditing and reporting compliance with this policy.

Freightways

Policy

Each **unit** must establish in consultation with **FIS** a documented procedure for approval of software acquisition outlining relevant business level approvers, evaluation criteria, compatibility with current standard operating environment where installation is required on to user endpoints and information security due diligence in the case of software as a service (Cloud Services)

Standard Operating Environments

- Documented **SOE** must be established for all end user endpoints.
- Documented **SOE** must be established for all application servers.
- The documented **SOE** must define the approved software and supported version within that environment.

SaaS / Software as a Service (Cloud Services)

- **Information security** due diligence must be undertaken of any new vendor/service provider– does the vendor/service provider have a current third-party audit report of their information security posture e.g. **ISO 27001, PCI-DSS, SOC2 Type II report**
    - Alternatively, the vendor should be asked to complete a risk assessment questionnaire for **FIS** Information Security team to evaluate.
- A privacy impact assessment (**PIA**) should also be considered if there will be any personally identifiable information held within this service either **Freightways** employees and/or **Freightways** client information. Guidance on this available via Office of the Privacy Commissioner in New Zealand and Office of the Australian Information Commissioner.

Protection of Intellectual Property Rights

The protection of intellectual property rights within operational jurisdictions of **Freightways units** must be upheld in line with applicable legislation, licensing and/or service agreements.

- Ensuring no unapproved software or unlicensed software is in use.
- No unauthorised duplication or distribution of software
- Ensuring approved software deployments are within licensed limits.

Other IT-related policies

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