IT and Cyber Security Policy

SAMPLE

Table of Contents

SAMPLE

SAMPLE

SAMPLE

Purpose

This IT and Cyber Security Policy sets out how [Company Name] manages information technology (IT) and cyber security risks to protect workers, contractors, customers, and visitors, and to support work health and safety (WHS) objectives. It applies to all workers, including employees, labour hire, contractors, volunteers, and visitors who access [Company Name] systems, whether in offices, retail stores, warehouses, or working remotely.

This policy aims to:

- Reduce WHS risks arising from IT and cyber security incidents, including stress, fatigue, and psychological harm.
- Protect confidential and sensitive information, including worker records and customer data.
- Ensure continuity of business operations for office, corporate, retail, and wholesale environments.
- Support compliance with relevant WHS, privacy, and cyber security requirements.

Scope

This policy applies to:

- All locations operated or controlled by [Company Name], including corporate offices, retail outlets, wholesale warehouses, and remote or home-based work locations.
- All IT assets owned, leased, or managed by [Company Name], including:
  - Desktop computers, laptops, tablets, and mobile phones.
  - Point of Sale (POS) systems and EFTPOS terminals.
  - Servers, cloud services, and network equipment.
  - Business software, email systems, and collaboration tools.
  - CCTV systems, access control systems, and other network-connected devices.
- All information handled by [Company Name], including:
  - Worker and contractor records.
  - Customer and supplier information.
  - Financial, sales, inventory, and operational data.
  - WHS records, incident reports, and safety documentation.

This policy operates alongside [Company Name]'s WHS Policy, Privacy Policy, Records Management Policy, and any relevant employment or contractor agreements.

SAMPLE

Definitions

Key Terms

- **Information Technology (IT)** – Hardware, software, networks, and systems used to store, process, or transmit information.
- **Cyber Security** – Measures used to protect systems, networks, and data from unauthorised access, damage, or disruption.
- **Information Asset** – Any data, record, file, or system that has value to [Company Name].
- **Personal Information** – Information about an identified individual or an individual who is reasonably identifiable.
- **Multi-Factor Authentication (MFA)** – A security process requiring two or more methods of verification to access systems.
- **Phishing** – A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity, often via email or SMS.
- **Malware** – Malicious software such as viruses, ransomware, or spyware that can damage or disrupt systems.
- **Remote Work** – Work carried out away from a [Company Name] site, including from home, client sites, or while travelling.
- **Critical System** – Any system whose failure would significantly impact safety, operations, or legal compliance (e.g. payroll, WHS incident reporting system, POS network).

WHS and IT / Cyber Security

IT and cyber security are directly linked to WHS. Cyber incidents can:

- Interrupt operations, creating stressful and unsafe working conditions.
- Compromise WHS records, incident data, or safety procedures.
- Lead to psychological harm, including anxiety, distress, or bullying and harassment through digital channels.
- Create physical safety risks if systems controlling access, alarms, or CCTV are compromised.

[Company Name] recognises that safe systems of work include safe and secure information systems. Cyber security controls are therefore treated as risk controls under WHS legislation and integrated into the organisation's risk management processes.

Responsibilities

Officers (e.g. Directors, Senior Managers)

Officers must exercise due diligence to ensure that [Company Name] has appropriate IT and cyber security systems in place to manage WHS risks. This includes:

SAMPLE