

# IT and Cyber Security Policy

SAMPLE

## Table of Contents

Purpose .....	5
Scope .....	5
Definitions.....	6
Key Terms .....	6
WHS and IT / Cyber Security .....	6
Responsibilities.....	6
Officers (e.g. Directors, Senior Managers) .....	6
Managers and Supervisors.....	7
IT Department / External IT Provider .....	7
Workers and Contractors.....	7
Visitors and Third Parties .....	8
Risk Management.....	8
Identification of IT and Cyber Risks .....	8
Risk Assessment.....	9
Example Risk Assessment Table .....	9
Risk Control and Hierarchy .....	9
Monitoring and Review.....	9
Access Control and User Management.....	9
User Accounts and Authentication.....	9
Password Requirements .....	10
Access Levels and Permissions .....	10
Termination and Role Changes .....	10
Use of Devices and Systems .....	10
Acceptable Use.....	10
Corporate and Office Environments .....	11
Retail and Wholesale Environments.....	11
Personal Use .....	11
Remote Work and Mobile Devices.....	11
Remote Work Requirements .....	11
Mobile Devices and Laptops .....	12

Bring Your Own Device (BYOD).....	12
Data Protection and Privacy .....	12
Data Classification and Handling.....	12
Personal and Health Information .....	12
Data Retention and Disposal.....	13
Email, Messaging, and Internet Use .....	13
Email Use.....	13
Messaging and Collaboration Tools.....	13
Internet Browsing .....	13
Cyber Threats and Incident Management.....	13
Types of Cyber Threats .....	13
Incident Reporting.....	14
Incident Response .....	14
Training, Consultation, and Communication.....	14
Training.....	14
Consultation.....	15
Communication.....	15
Psychological Health and Online Behaviour.....	15
Respectful Online Conduct.....	15
Managing Stress from Cyber Incidents.....	15
System Acquisition, Change, and Maintenance .....	16
Procurement and Implementation .....	16
Change Management.....	16
Patching and Updates.....	16
Backup, Recovery, and Business Continuity .....	16
Backups .....	16
Recovery and Business Continuity.....	16
Monitoring, Audits, and Continuous Improvement.....	17
Monitoring .....	17
Audits.....	17
Continuous Improvement .....	17
Checklists .....	17

Worker IT and Cyber Safety Checklist..... 17

Manager / Supervisor Implementation Checklist..... 18

Policy Review and Document Control ..... 18

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

- 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.

## 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 or 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: