Cyber Security Incident Response Plan

Table of Contents

Purpose and Scope

This Cyber Security Incident Response Plan sets out the arrangements [Company Name] will use to prepare for, detect, respond to and recover from cyber security incidents that may impact work health and safety (WHS), business continuity, personal information and critical services.

The plan applies to all workers, including employees, contractors, volunteers and labour-hire staff engaged by [Company Name] in:

- Office and corporate environments (e.g. head offices, administration centres, professional services)
- Retail and wholesale operations (e.g. point-of-sale systems, inventory systems, online stores)
- Disability and aged care services (e.g. client management systems, care planning systems, telehealth, medication management and rostering systems)

This document should be read in conjunction with [Company Name]'s:

- WHS Policy
- Risk Management Procedure
- Information Security Policy
- Business Continuity Plan (BCP)
- Privacy and Confidentiality Policy

The primary objectives of this plan are to:

- Protect the health, safety and welfare of workers, clients, residents, visitors and others who may be affected by a cyber incident
- Minimise disruption to critical business and care services
- Protect the confidentiality, integrity and availability of information assets
- Support compliance with WHS, privacy and other relevant legislation and standards
- Enable timely, coordinated and well-documented responses to cyber incidents

Definitions

For the purposes of this plan, the following definitions apply:

- **Cyber security incident** – Any actual or suspected event that compromises, or threatens to compromise, the confidentiality, integrity or availability of information, information systems, or supporting infrastructure. This includes events that disrupt safe work systems or care delivery.
- **Notifiable data breach** – A data breach that is likely to result in serious harm to individuals, requiring notification under the Privacy Act 1988 (Cth) Notifiable Data Breaches (NDB) scheme.

- **Critical systems** – Systems that are essential to safe operations, care delivery or legal compliance, such as client/resident management systems, medication management systems, payroll, rostering, point-of-sale (POS) systems, and building access control.
- **Incident response** – The organised approach to managing and addressing the consequences of a cyber security incident, including containment, investigation, communication, recovery and post-incident review.
- **Malware** – Malicious software designed to disrupt, damage or gain unauthorised access to systems or data (e.g. ransomware, viruses, trojans).
- **Phishing** – Fraudulent attempts, usually by email, SMS or messaging, to obtain sensitive information or install malware by pretending to be a trustworthy entity.
- **Denial of Service (DoS/DDoS)** – An attack designed to make a system or service unavailable to its intended users.
- **Personal information** – Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

Legislative and Standards Context

[Company Name] must ensure, so far as reasonably practicable, that cyber risks which may impact health and safety are identified, assessed and controlled in line with WHS legislation and other relevant laws. This includes:

- Work Health and Safety Act and Regulations (jurisdiction-specific)
- Privacy Act 1988 (Cth) and Notifiable Data Breaches scheme
- Aged Care Act 1997 and associated Quality Standards (for aged care providers)
- NDIS Act 2013 and NDIS Practice Standards (for disability service providers)
- Fair Work Act 2009 (in relation to payroll and worker records)
- Applicable State/Territory health records and information privacy legislation

Relevant guidance and standards include:

- Australian Cyber Security Centre (ACSC) guidance and Essential Eight
- ISO/IEC 27001 Information Security Management Systems (where adopted)
- OAIC guidance on data breach preparation and response

This plan supports WHS duties by ensuring that cyber incidents which may compromise safe systems of work, emergency response, medication management, financial systems or access to premises are managed in a structured, timely and competent manner.

Roles and Responsibilities

Officers (e.g. Board Members, Executives)

Officers of [Company Name] must exercise due diligence to ensure that cyber risks with WHS implications are properly managed. This includes:

- Ensuring adequate resources are available for cyber security, including staff, training, tools and external support
- Approving and periodically reviewing this Cyber Security Incident Response Plan
- Ensuring cyber security risk is integrated into WHS risk management, business continuity and governance processes
- Monitoring cyber security performance and incident trends

Senior Management

Senior managers (e.g. General Managers, Service Managers, Store Managers) are responsible for:

- Implementing this plan within their area of control
- Ensuring workers are trained in incident reporting, basic cyber safety and emergency procedures
- Ensuring critical systems in their area (e.g. POS in retail, client management in disability/aged care, payroll in corporate offices) are identified and documented
- Ensuring incident response activities are coordinated with WHS and emergency management procedures

IT / Cyber Security Team

The IT or managed service provider (MSP) responsible for [Company Name]'s systems must:

- Maintain technical controls to detect, contain and eradicate cyber incidents
- Lead the technical aspects of incident response, investigation and recovery
- Maintain system logs, backups and monitoring tools
- Provide timely technical advice to management and the Incident Response Team (IRT)
- Maintain an up-to-date inventory of systems, applications and data repositories

Work Health and Safety Representatives and Committees

WHS representatives and committees must:

- Consider cyber-related WHS risks (e.g. disruption to duress alarms, access control, emergency communications) in consultation processes