# Information Security Policy

V.2025.08

**PowerHouse Hub**
Building 6, 2440 Logan Road
Eight Mile Plains QLD 4113
www.powerhousehub.com
+61 (0)7 3518 4020

# Version Information

| Version | Date | Update | Author / Reviewers | Approved by |
|---|---|---|---|---|
| V 2.05 | Apr, 2021 | Annual Review and update | Philip Atkinson | Tony Carrucan |
| 2023 | Feb, 2023 | Annual Review and update | Philip Atkinson | Tony Carrucan |
| 2023.4 | April, 2023 | Additional updates | Philip Atkinson | Tony Carrucan |
| 2024.11 | Nov, 2024 | Annual Review and update | Philip Atkinson | Tony Carrucan |
| 2025.08 | Aug, 2025 | Annual Review and update | Philip Atkinson | Tony Carrucan |

# Contents

# Purpose

The purpose of this policy is to establish the framework for protecting the confidentiality, integrity, and availability of the company's information assets.

# Scope

This policy applies to:

- All employees, contractors, and third parties who access company systems, data, or facilities.
- All information assets owned, managed, or processed by the company, including digital, paper-based, and intellectual property.
- All systems, networks, cloud services, and devices used to store, process, or transmit company data.

# Policy Statement

The company is committed to:

- Protecting information assets from all threats, whether internal or external, deliberate or accidental.
- Ensuring compliance with applicable legal, regulatory, and contractual requirements.
- Maintaining business continuity and minimising the impact of security incidents.
- Continual improvement of the IMS through monitoring, audits, and management reviews.

# Objectives

The objectives of this policy are to:

1. Ensure information is classified, handled, and protected according to sensitivity.
2. Control access to information and systems based on business and security requirements.
3. Protect against unauthorised access, disclosure, alteration, and destruction of information.
4. Establish processes for incident management, response, and recovery.
5. Educate employees and contractors on their security responsibilities.
6. Regularly assess risks and apply appropriate controls.

# Roles and Responsibilities

- **Top Management**: Approve and support the IMS, provide resources, and review performance.
- **Chief Information Security Officer (CISO)**: Oversee IMS implementation, risk management, awareness, and compliance.
- **Managers**: Ensure their teams comply with this policy and apply security controls.
- **Employees & Contractors**: Follow security procedures, report incidents, and protect company data.
- **Third Parties**: Must comply with contractual information security requirements.

# Information Security Principles

- **Confidentiality**: Information is accessible only to authorised individuals.
- **Integrity**: Information is accurate, complete, and protected from unauthorised modification.
- **Availability**: Information and systems are accessible when required by authorised users.

# Access Control

- Access to systems and information will be based on the principle of least privilege.
- User accounts must be unique and protected with strong authentication methods.
- Privileged access must be monitored and periodically reviewed.

# Risk Management

- Risks to information assets must be identified, assessed, and treated in line with the risk management register.
- Risk assessments will be reviewed regularly and following significant changes.

# Incident Management

- All employees must report actual or suspected information security incidents immediately.
- The CISO will ensure proper investigation, mitigation, and reporting of incidents.
- Lessons learned will be used to improve controls and processes.

# Compliance

- All staff must comply with this policy and related procedures.
- Breaches may result in disciplinary action, up to and including termination of employment.
- The company will comply with all applicable data protection and privacy laws.

# Monitoring and Review

- The effectiveness of this policy and the IMS will be reviewed annually by top management.
- Regular internal audits and management reviews will ensure continual improvement.