SWSPHN Policy

Information Security Policy

Purpose

This policy defines the purpose, direction, principles and basic rules for information security management.

Policy

South Western Sydney PHN (SWSPHN) is committed to understanding and effectively managing risks related to Information Security to provide greater certainty and confidence for our security holders, employees, customers, suppliers and the communities in which we operate. Finding the right balance between Information Security risk and business benefit enhances our business performance and minimises potential future exposures.

This policy applies to all information, computer and network systems governed, owned by and/or administered by SWSPHN.

It is the policy of SWSPHN to ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be maintained
- Information will not be disclosed to unauthorised persons through deliberate or careless action
- Integrity of information is maintained through protection from unauthorised modification
- Availability of information to authorised users when needed
- All staff complete Information Security training
- All suspected breaches of Information Security will be reported and investigated

Any individual dealing with information at SWSPHN, no matter their status (e.g. employee, contractor, or consultant), must comply with the Information Security policies and related documents.

1. Aims

The aims of our Information Security policies are to:

- Remain committed to satisfying all applicable requirements concerning information security, including:
    - Comply with all legal requirements, including relevant codes of conduct and legislation.
    - Comply with requirements of regulatory authorities, both internal and external.
    - Comply with contractual requirements, both internal and external.
    - Comply with industry best practices concerning information security controls.
- Remain committed to continuous improvement to increase our information security system effectiveness over time.

- Provide information security awareness training to employees to ensure they are adequately equipped to handle information security assets and other confidential information.
- Ensure information security risk assessments and objectives are established for all projects and services provided to clients before work commences.
- Information security incidents are investigated proportionate to their severity and impact, and reported to relevant authorities where required
- Use information security risk awareness and tolerance in our decision-making.
- Assess and treat all information security risks as quickly as possible.
- Protect all information security assets and confidential information entrusted to us using appropriate, industry-recognised security controls and systems.
- Manage, assess and treat information security risks within the business to an acceptable level via adequate design, implementation and maintenance of processes and information security controls
- Establish and maintain an effective Information Security Management System (ISMS) and use the international framework (ISO 27001) and required controls to provide the most secure environment for our operations.

2. Responsibilities

SWSPHN will:

- Encourage all employees and contractors to identify information security risks
- Encourage all employees and contractors to identify areas where improvement can be achieved
- Remove wasted and non-value-added steps and time in our processes where feasible
- Support the adoption of appropriate systems and management principles so that all stakeholders benefit from this commitment to information security

Employees are expected to:

- Assist and cooperate in ensuring that this policy is followed
- Actively participate in the adherence to this company policy and contribute to the achievement of the goals and objectives of this policy
- Assist and cooperate in ensuring that the Information Security policies are followed
- Report perceived and actual information relating to Information Security breaches and/or IT incidents either to the Executive Team or to their immediate Manager
- All employees are responsible for embedding information security risk management in our core business activities, functions and processes. Information security risk awareness and our tolerance for risk are key considerations in our decision making.

3. Objectives Framework

In implementing an Integrated Management System (IMS), the application of SMART goals is essential for setting robust and effective information security objectives:

- Specific: Each goal is defined with precision, outlining clear actions and expectations in the context of information security.
- Measurable: Goals are quantifiable, allowing for tracking and assessment of progress towards achieving specific information security outcomes.
- Achievable: Objectives are realistic, considering the organisation's resources and capabilities, ensuring they are within reach.
- Relevant: Each goal aligns with the broader information security needs and the strategic direction of the organisation, ensuring that they contribute meaningfully to overall information security.
- Time-bound: Goals have clear deadlines, providing a timeframe for achievement and review, which helps in maintaining focus and ensuring timely progress.

By strictly adhering to these SMART criteria, information security objectives become actionable and practical, significantly enhancing the organisation's information security posture in compliance with relevant standards. This approach not only ensures the effectiveness of the IMS but also supports its continual improvement.

4. Objectives

SWSPHN's information security objectives can be found in the Objectives List in SharePoint.

5. Information Security Change Management

SWSPHN ensures that all changes to information systems, services, infrastructure, and access controls that may affect information security are planned, assessed, approved, implemented, and recorded in a controlled manner. As a minimum, information security relevant changes must follow these steps:

1. Initiation - Change request submitted and documented.
2. Review – Security and technical evaluation completed, including risk and impact assessment.
3. Approval – Authorisation obtained from the appropriate authority prior to implementation.
4. Execution - Approved change implemented and actions recorded.
5. Verification - Confirm the change achieved its intended outcomes and that security controls remain effective.
6. Closure - Update records/documentation and capture lessons learned where applicable.

Emergency changes may be implemented to restore service or address an immediate security risk; however, they must be documented and undergo retrospective review and approval as soon as practicable.

This requirement applies to ICT, system owners, administrators, and any staff or third parties involved in initiating or implementing changes.

Applicability

All SWSPHN staff. This document is applied to all documents and records related to the IMS scope. Users of this document are all employees and relevant external parties.

Associated Documents

Legislation and best practice guidelines:

- Health Records and Information Privacy Act 2002
- ISO 27001 Information security management systems - Requirements
- Privacy Act 1988 – The Australian Privacy Principles (APPs)
- Privacy Amendment (Notifiable Data Breaches) Act 2017

Internal policies and documents:

- Access Control Policy and Procedure
- Asset Management Policy and Procedure
- Business Continuity and Disaster Recovery Plan Compliance Policy and Procedure
- Cyber Security Strategy
- Cyber Security Incident Response Plan
- Data Governance Framework
- Encryption and Cryptographic Controls Policy and Procedure
- Improvement and Corrective Actions Policy and Procedure
- Improvement and Corrective Actions Register
- Information Asset Register
- Information Classification and Handling Policy and Procedure
- Information Security Risk Register
- Information Security Objectives
- IT Acceptable Use Policy and Procedure
- Network Security Policy and Procedure
- Risk Management Framework
- Software Management Policy and Procedure
- Supplier Access and Security Policy and Procedure
- Supplier Register

Roles and Responsibilities

Document Owner	Ensure that this document is published and implemented, progress is monitored and that it is reviewed according to the document control schedule outlined in the document.
Approver	Provide advice to the document owner, approve the final document and present it to Senior Staff Meeting for approval.
Board	Exercise due diligence by ensuring SWSPHN meets legislative and compliance requirements.
Executive and Management	Ensure effective management of information and knowledge across the organisation and their portfolio areas.
Executive Corporate Services	Ensure SWSPHN adheres to its processes for managing risks to information confidentiality, integrity, and availability.
Data Custodian/ Privacy Officer	Ensure the safe storage, secure management and protection of data within SWSPHN. Ensure the organisation complies with data privacy laws and regulations.
Information Security Committee	Contribute expertise to the organisation's overall information security posture.
SWSPHN Staff	Comply with this policy and associated legislation.

Definitions

View related definitions in the Integrated Management System (IMS) Glossary.

Document Control

Document review every (choose most applicable) ☐ 1 year ☐ 2 years ☑ 3 years

Version	Date Commenced	Document Owner	Change Description	Review Date	Approver
V1.0	August 2025	IT Manager	New Policy	August 2028	Executive Manager Corporate Services
V2.0	February 2026	Executive Manager Corporate Services	Policy update – inclusion of change management process	February 2029	CEO

This document will remain in effect until replaced.