SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	Information Security Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/310
DATE OF PUBLICATION	August 2019
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Standard 1: Clinical Governance ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems.
REVIEW DATE	August 2024
FORMER REFERENCE(S)	SESLHDPD/278 Information Security (including Digital Information Asset Security Policy)
EXECUTIVE SPONSOR or **EXECUTIVE CLINICAL SPONSOR**	Flora Karanfilovski SESLHD Director Information Management Services Directorate
AUTHOR	Program Manager ICT Security and Strategy Information Management Services Directorate
POSITION RESPONSIBLE FOR THE DOCUMENT	Jon Straker Deputy ICT Director
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance
SUMMARY	This document provides the overarching policy under which digital information should be handled at South Eastern Sydney Local Health District.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

Feedback about this document can be sent to seslhd-executiveservices@health.nsw.gov.au

1. POLICY STATEMENT

South Eastern Sydney Local Health District (SESLHD) recognises that ownership of the records of care provided to a patient (Personal-Health-Information) and information on supporting systems is often a contentious issue. As stewards of this private and confidential information, SESLHD has a primary responsibility to ensure that they maintain the security and integrity of the data.

SESLHD also has a responsibility to ensure that Personal-Health-Information records are used in a way that a patient would reasonably expect to be necessary to support their care.

The policy further recognises that broad clinical access to patient records is necessary for the safe and effective functioning of an evidence based integrated healthcare system.

SESLHD has a duty of care and a legislative requirement, to their staff and the community at large, and there will be occasions when confidential and sensitive information must be shared to meet this duty of care. In these circumstances the policy ensures that appropriate controls, review and audits are in place to be able to monitor and manage digital information access.

2. AIMS

The purpose of the Information Security Policy is to provide the principles used to manage and protect SESLHD digital assets and is the key policy of the Information Security Management System (ISMS).

The Information Security Policy specifies principles that:

- Examines the organisation's information security risks, taking account of internal and external threats, system vulnerabilities, and probable impacts to SESLHD
- Implements an information security design which will produce a coherent and comprehensive suite of information security controls and/or forms of risk treatments (such as risk avoidance or risk transfer) to address risks that are deemed unacceptable
- Adopts governance that is to guide information security policies, process and controls to meet SESLHD’s digital information security needs on an ongoing basis.

The Information Security Policy is a primary policy supported by several technical information security policies which should not be considered in isolation but together and shall have equal standing.

2.1 Information Security Policy Scope

The policy applies to all digital information held in any electronic form. No distinction is made as to the electronic medium on which the information is stored as the policy is intended to be technology independent.

Where ambiguity exists regarding the use of, or access to, Personal-Health-Information, an initial consultation with the SESLHD Information Security Governance Committee (ISGC) must occur to gain clarity with the intent of avoiding an adverse impact on the care.

The ISMS is the framework which includes a collection of policies, processes and other documents that consists of:

- Business, ICT and ISMS strategies;
- Security Governance;
- Policies covering all aspects of information security;
- Processes and procedures that have an information security component;

- Controls and standards;
- Metrics and measurements;
- Roles and responsibilities;
- Risk Management; and
- Continuous improvement program.

As the Information Security Policy is part of a framework, the diagram in Appendix 1 - Information Security Management System architecture – ISMS, shows the context and the interrelationships between each of the artefacts. The understanding of the framework is critical to understanding the accountability and responsibility placed upon SESLHD staff as facilitators in maintaining the security of digital assets.

This document is the prime policy which supports the governance of information security and dictates the principles upon which Information Security is to be managed to support the Confidentiality, Integrity and Availability (CIA) and meet the compliance and assurance as required by the NSW Government Cyber Security Policy.

2.2 Information Security Policy Exemptions

Any exemptions to the Information Security Policy or associated technical policies must be approved by the Chief Information Officer (CIO) or designated Senior Information Security Officer (SISO) after a risk assessment has been completed, reviewed and approved by the Information Security Governance Committee (ISGC). Written approval for exemption must be completed through a brief and must be recorded within the Document Management System (i.e. Content Manager) in line with records management policies.

2.3 INFORMATION SECURITY GOVERNANCE

Information Security Governance Objective

Information Security (IS) Governance ensures that business and stakeholder needs, conditions and options are evaluated to determine the alignment to the organisational business strategy. This sets direction through prioritisation and decision making whilst monitoring performance and compliance against agreed objectives.

Information Security Governance Scope

Information Security Governance must be applied to digital systems regardless of their size, criticality or type. The delivery of the governance can be done through either a representative body or via joint management/ team leadership.

The district has established an Information Security Governance committee (ISGC).

The Information Security Governance Committee

The ISGC provides oversight on Information security matters and an avenue for district staff to raise information security risks and guidance. The responsibilities and duties are outlined in the ISGC terms of reference T18/8584.

2.4 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

Training and Awareness Objective

The purpose of information security training is to provide assurance that all staff, have awareness of what information security is and how they can assist in safeguarding the SESLHD digital assets. Staff must demonstrate the appropriate skills and competencies to warrant that all activities are completed successfully and correct decisions are made.

All employees within SESLHD and, where relevant, contractors must receive appropriate awareness education, training and regular updates in organisational policies and procedures, as relevant for their job function.

Training and Awareness Scope

Staff must be provided access to information security training at the commencement of their employment with refresher updates annually. Training can be delivered by any communication avenue that will support the organisation in gaining awareness. Awareness of the SESLHD Information Security Policy must be brought to the attention of and made available to all authorised users.

In addition to information security training on the correct application to ICT facilities and applications, users must be equipped to support the SESLHD Information Security Policy in the course of their normal work. Users of SESLHD digital assets must not subvert SESLHD information security measures.

2.5 INFORMATION SECURITY RISK MANAGEMENT

ISMS Risk Objective

Risk management provides the ability to assess the value and priority of potential threats and identify mitigating actions to reduce a risk to acceptable tolerances. The application of risk management is a mandatory requirement of the NSW Government as part of the DISP and for SESLHD it is formalised within Risk Management – Enterprise Risk Management Policy and Framework - NSW Health PD2015_043, and SESLHDPR/304 - Enterprise Risk Management System (ERMS) Procedure.

SESLHD departments and ICT service providers that manage digital assets must adopt risk management practices to cover all areas of information security activities across the organisation based upon the NSW Health Framework, NSW Government Risk Management guidelines TPP12-03b and supported by AS/NZS ISO31000:2009.

ISMS Risk Management Scope

SESLHD departments and ICT service providers that host digital assets must utilise the approved NSW Health Risk Management Framework and ISO31000 Risk Management Principles and Guidelines as a reference when selecting and implementing information security controls, and in evaluating and treating information security risks as part of a formal risk management process.

2.6 INFORMATION SECURITY IN PROJECT MANAGEMENT

ISMS Project Management Objective

Information Security must be addressed in project management, regardless of the type of the project.

ISMS Project Management Scope

Information Security must be integrated into all projects to ensure that information security risks are identified and addressed as part of a project. This applies to all projects regardless of character, e.g. a project for a core business process, ICT, facility management and other supporting processes.

The project management must ensure that:

- Information security is included in project objectives;
- An information security risk assessment is conducted at the commencement of the project to identify necessary information security controls;
- That the risk posture is determined and documented;
- Information security is part of all phases of the applied project methodology;
- A risk assessment is conducted at stage gates or when appropriate to ensure that the risks are current and to capture any new risks;
- Any business processes that are identified for change are considered in view of information security;
- A Security Management plan is developed;
- Security acceptance testing is conducted; and
- Security certificates are issued prior to go-live.

2.7 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Information Security Roles & Responsibilities Objectives

Oversight of Information Security is required to provide assurance that the information security controls are being appropriately applied and monitored. Two key factors in delivering Assurance is the role of a Responsible Offices and that systems administration roles are separated from Information Security roles.

Responsible Officer

SESLHD must appoint a Senior Responsible Officer (SRO) who acts as the central point of contact for oversight, risks, issues, provides advice and other aspects relating to Information Security.

Information Security Roles & Responsibilities Scope

Roles and responsibilities relating to positions that have an information security impact must be separated from daily administration duties which should be applied as practicable.

The defining of roles, responsibilities and structure must be in alignment with the NSW Government Cyber Security Policy and ISO/IEC 27001:2013(E) Section 5.3.

Where the segregation of duties are be difficult to achieve or costly, mitigating controls must be employed such as monitoring of activities, audit trails and management supervision.

2.8 INFORMATION SECURITY DOCUMENTATION

ISMS Security Documentation Objective

Information Security documentation must accompany all services so that compliance and risk assessments can be conducted. The documentation is to outline the security posture of the application or service in its default configuration and steps required to meet the SESLHD minimum set of Information Security standards.

ISMS Information Security Documentation Scope

All ICT services within SESLHD and must adhere to the Information Security minimum requirements. Information Security documents must be available for ICT services and must be available before the services / system goes live.

SESLHD Departments and ICT service providers shall determine the boundaries and applicability of the information security to establish if the scope has been met in alignment with the DISP. The documents must be available in either MS Word or PDF format.

Information Security Management Plans

All services must have an Information Security Management Plan (ISMP) accompanying the security information documentation that governs the integrity, privacy, security, and confidentiality of information, especially highly sensitive information, and the responsibilities of departments and individuals for such information.

2.9 CORPORATE AND CLINICAL APPLICATIONS

Corporate and Clinical Applications Objective

To ensure that the information system security requirements of corporate and clinical applications are considered, assessed, documented and applied as part of the lifecycle of applications.

Corporate and Clinical Applications Scope

For all corporate and clinical applications the analysis of the information security requirements must form part of any proposal prior to acquisition. The end state system must comply with the SESLHD Information Security Policy, the NSW Government DISP and ISO27001 requirements. Corporate and Clinical Applications (C&CA) that are in Business as Usual (BAU) mode, must undergo a risk assessment and security posture documented for ISGC review and risk acceptance. If the risk tolerance is outside the corporate or department limits, then mitigation actions must be taken to bring the application or system within tolerance, this may include replacement.

The security requirements and controls should reflect the value of the information involved, and the potential damage which might result from a failure or absence of security.

2.10 SYSTEMS SURVEILLANCE AND MONITORING

Systems Surveillance and Monitoring Objective

System monitoring must be defined and operated to ensure a system remains compliant with this policy, the NSW Government DISP and ISO2700 Information Security Standard.

Systems Surveillance and Monitoring Scope

Information Systems should be monitored to ensure conformity with security standards of Confidentiality, Integrity and Availability (CIA). In order to have effective monitoring and audit tools, it is essential that logging of potentially damaging events including; exceptions, violations and other security-relevant events, be performed, monitored and retained for a period of time. Where possible, event logs should include User IDs, dates and times, and node address or terminal identifier.

Monitoring should be integrated at the planning, design and implementation stages of a project. Information security procedures and controls capable of enabling prevention, prompt detection of security events, and response to security incidents must be included in the project plan.

2.11 MALICIOUS SOFTWARE MITIGATION

Malicious Software Mitigation Objective

To ensure that information, and information processing facilities, are protected against malicious software or malware.

Malicious Software Mitigation Scope

Mitigation actions must detect, prevent and provide recovery controls to safeguard against malicious software and should be combined with appropriate user awareness.

All digital assets must be protected and the following guidance should be considered:

- Conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorised amendments should be formally investigated
- Installing and ensuring regular updates of malware detection and repair software that will scan digital assets and media as a precautionary control on a routine basis. Scanning to be applied to:
    - Any files that are received over networks or via any form of storage medium
    - Electronic mail attachments and downloads
    - Web pages.
- Scanning at different places, e.g. at electronic mail servers, desktop computers and at network entry points
- Defining procedures and responsibilities to deal with malware attacks on digital assets
- Preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements
- Implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware
- Implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative
- Isolating environments where catastrophic impacts may result.

It is essential that precautions are taken to prevent and detect the currently known forms of malicious software and computer viruses on digital assets which will require planned and tested processes for distributing updates to resolve identified system vulnerabilities.

Virus detection and prevention measures must be implemented on all digital assets including mobile and smart devices that come in contact with SESLHD infrastructure. Users must be made aware of cyber threats and their responsibilities through awareness campaigns or training.

2.12 ISMS COMPLIANCE WITH LEGAL REQUIREMENTS

All relevant contractual and statutory requirements must be explicitly defined and documented for each digital asset, and the specific controls and responsibilities to meet these requirements must be defined and documented in the digital asset management plan.

Proprietary software products are usually supplied under a licence agreement that limits the use of the product to specific computers. Users of the software must be aware of the limitations imposed by the licence agreement and comply with them.

A register of software must be maintained for all digital systems and regular audits of software use must be undertaken. Audits may be conducted by the business managers of the application, service providers or external / internal auditors. Users must not copy software from one computer to another without the consent of the software owner.

Vendor Compliance

Vendors who are certified on the NSW Government Tender Panel must comply with;

- NSW Government Cyber Security Policy
- NSW Government Cloud Policy
- Australian Cyber Security Centre’s (ACSC) Essential 8
- All other applicable NSW Government policies, and
- SESLHDPD/310 Information Security Policy and SESLHD supporting technical policies.

The compliance is referenced in Schedule 1 of the General Order Form, Procure IT Version 3.2, Item 25. Secrecy and Security.

Vendors engaging in supplying digital services with South Eastern Sydney LHD must comply with the above mentioned policies and the SESLHDPD/318 - Vendor Compliance Policy.

District and Department Compliance

Strong cyber security is an important component of the NSW Digital Government Strategy. The NSW Government has mandated the NSW Cyber Security Policy as the minimum set of information security controls that must be met by Government agencies and their departments.

Departments that manage or host their own digital infrastructure and systems must meet the controls set out in this policy and in the NSW Cyber Security Policy. The NSW Cyber Security Policy references the following standards as a baseline for compliance and assurance;

- ISO27001:2013 for general governance and operational risk;
- ISA/IEC62443 for Internet of Things devices; and
- ACSC Essential 8 for securing systems in general.

Managers of digital systems must review the NSW Cyber Security Policy for applicability to their systems and if assistance is needed in attaining compliance, they can seek guidance from Health ICT by lodging a request via the eHealth State Wide Service Desk or SARA.

3. TARGET AUDIENCE

The policy applies to permanent, temporary and casual staff of SESLHD, staff seconded from other organisations, contingent workers including labour hire, service providers, professional services contractors, consultants and volunteers who may utilise SESLHD infrastructure and/or access SESLHD information systems and applications (including systems provided by external providers such as eHealth) with respect to the security and privacy of information.

All staff are responsible for information security and must comply with this policy, the supporting ISMS technical policies and NSW Health Code of Conduct.
Failure to comply with policy may result in disciplinary action.

4. DEFINITIONS

ISMS: The Information Security Management System (ISMS) is a framework that contain policies and procedures for tackling security risks in an organisation. The focus of an ISMS is to ensure business continuity by minimising all security risks to information assets and limiting security breach impacts to a minimum.

DISP: The Digital Information Security Policy (DISP) sets out the digital information security requirements for the NSW public sector as mandated by the NSW Government.

ISO27001: ISO/IEC 27001:2013 is an information security standard that provides a framework for an Information Security Management System (ISMS).

BAU (Business as Usual): the daily operational activities to maintain information systems.

CIA Triad: The CIA Triad of information security is an information security benchmark model used to evaluate the information security of an organisation. The CIA Triad of information security implements security using three key areas related to information systems including confidentiality, integrity and availability.

5. DOCUMENTATION

N/A

6. REFERENCES

Policies and Guidelines

- NSW Government Cyber Security Policy
- NSW Government ICT Strategy
- NSW Ministry of Health Policy Directive PD2013_033 - Electronic Information Security Policy - NSW Health
- NSW Ministry of Health Policy Directive PD2015_043 - Risk Management - Enterprise-Wide Risk Management Policy and Framework - NSW Health
- NSW Information Classification and Labelling Guidelines
- SESLHDPD/318 – Vendor Compliance Policy
- SESLHDPR/304 - Enterprise-wide Risk Management System - ERMS
- SESLHD ISMS Strategy 2017-2022

Legislation

- Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)
- Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
- Government Information (Public Access) Act 2009 (GIPA Act)

Standards

- ISO 27001:2013 Information technology - Security techniques - Information security management systems.
- ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management.
- ISO 27014 Information technology – Security techniques – Governance of information security
- ISO 31000 Risk management - Principles and guidelines
- ISO/IEC 38500:2015 Information technology - Governance of IT for the organisation

Supporting Documentation

- Australian Government Cyber Security Strategy
- Australian Signals Directorate: Australian Government Information Security Manual
- Australian Signals Directorate: Strategies to Mitigate Targeted Cyber Intrusions
- Australian Signals Directorate: Top Four Mitigation Strategies to Protect Your ICT System
- Australian Government Attorney-General's Department Protective Security Framework
- Cobit 5 for Information Security
- ISACA Overview of Digital Forensics

7. REVISION AND APPROVAL HISTORY

Date	Revision No.	Author and Approval
May 2018	DRAFT	Shane Feeney Program Manager ICT Security & Strategy. Flora Karanfilovski Director, Health ICT
October 2018	DRAFT	Processed by Executive Services prior to submission to SESLHD Executive Council
November 2018	0	Approved by Executive Council
August 2019	1	Minor review updating references and hyperlinks drafted by Shane Feeney and Richelle Risi. Approved by Executive Sponsor. Formatted by Executive Services prior to publishing.

Appendix 1. ISMS Overview

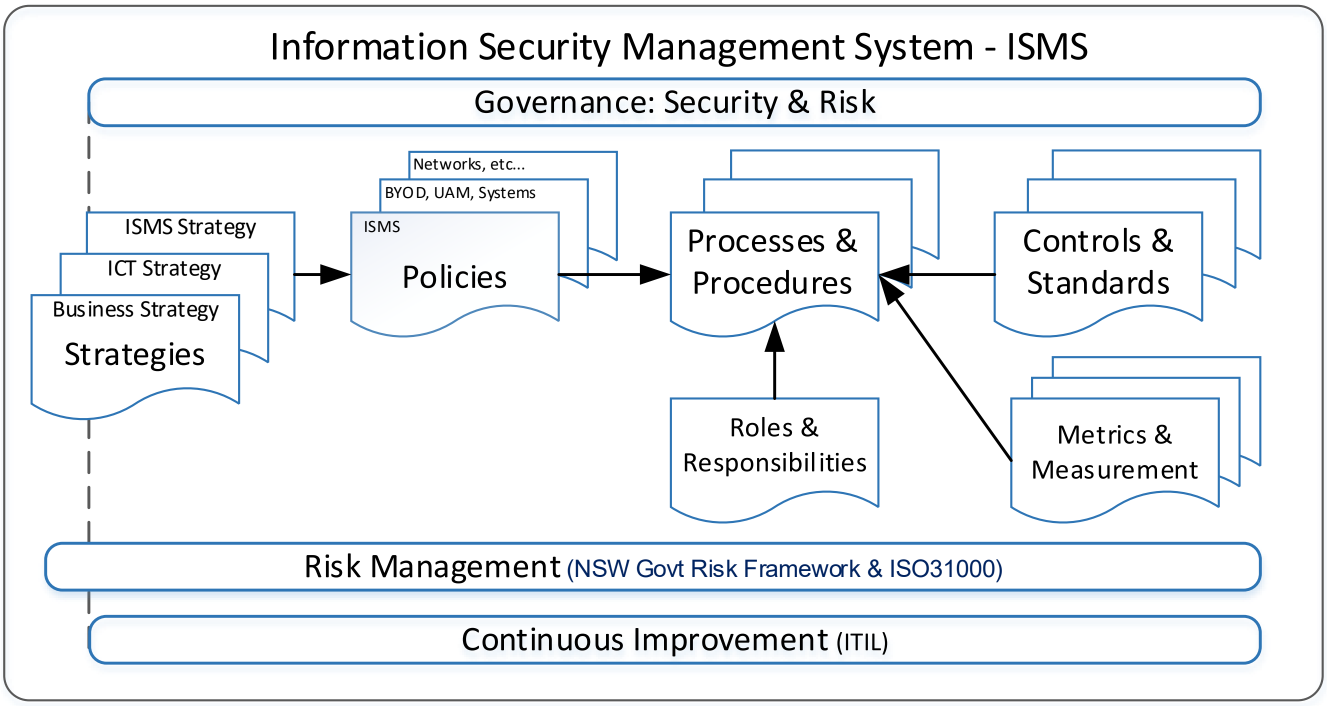

Figure 1. Information Security Management System architecture – ISMS