SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	System Accreditation Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/316
DATE OF PUBLICATION	June 2019
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Standard 1 – Governance for Safety and Quality in Health Service Organisations ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems.
REVIEW DATE	June 2024
FORMER REFERENCE(S)	None
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Flora Karanfilovski Director, Health ICT Directorate / CIO, SESLHD
AUTHOR	Shane Feeney
POSITION RESPONSIBLE FOR THE DOCUMENT	Program Manager, ICT Security & Strategy Health ICT Shane.Feeney@health.nsw.gov.au
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance.
SUMMARY	This document provides the overarching policy which information systems should be accredited for use at South Eastern Sydney Local Health District.

Systems Accreditation Policy SESLHDPD/316

1. POLICY STATEMENT

The security of South Eastern Sydney Local Health District (SESLHD) information is critical to meeting our information security obligations and to ensure the resilience and ongoing success of SESLHD.

The Systems Accreditation Policy addresses the risk the SESLHD infrastructure is exposed to when a new system is connected to the SESLHD digital infrastructure. Past experience has shown that systems which do not undergo certification prior to attachment, have caused significant disruption to the operation of the district.

The policy focuses on establishing a trusted environment through accrediting systems, which includes hardware and software and leverage off information security mechanisms towards providing a trusted, safe, secure, compliant and best practices environment.

2. AIMS

The purpose of the Systems Accreditation (SA) Policy is to describe the principles used to manage and protect SESLHD digital infrastructure from deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss or use.

This policy applies to all systems and services that meet the definition of a service as outlined in **Section 4 - Definitions.**

3. TARGET AUDIENCE

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

4. POLICY SCOPE

A system is a regularly interacting or interdependent group of items, forming a unified whole, is/will be offered as a service and can comprise of;

- Applications either custom built or Out of the Box (OOTB);
- Servers (hardware) and operating systems;
- Cloud services such as Azure/ Amazon Web Services; or
- All of the above.

All ICT systems must undergo the Health ICT system accreditation procedure. To engage Health ICT (HICT) to assist with the accreditation of your system, please log a request with the eHealth State Wide Service desk (SWSD).

The system accreditation procedure can be found on the SESLHD intranet under Support & Corporate Services page, Health ICT page then Processes.

4.1 Logging and Monitoring

Event logging and monitoring standards are to be applied and tested to the system prior to deployment. The administrator and information asset owner must define the standards of logging required for the system.

4.2 Cryptographic Key and Certificate Management

If cryptography is used by the system, then processes must be implemented to protect cryptographic materials and prevent unauthorised access to or distribution of them.

In addition, processes must be in place to ensure that all relevant cryptographic materials are revoked and/or renewed at the appropriate time.

4.3 Auditing

The system administrator must ensure the audit function enables collection and security of audit evidence as per the requirements identified in Security Risk Assessment (SRA).

4.4 Security Technology

If the system is using any security technology component (e.g. security token, mobile terminal, etc.), the security technology must be registered with Health ICT, management and revocation of this component must be possible.

4.5 Backup and restore

System administrators must ensure that the system and related middleware and databases are properly backed up and completely recoverable in accordance with meeting business and legal requirements.

4.6 Exemptions

Any exemptions to the Systems Accreditation Policy must be approved by the District Chief Information Officer (CIO), or SESLHD ICT Deputy Director after a risk assessment has been completed. Written approval for exemption must be completed via a brief and must be recorded within the document management system (i.e. Content Manager) as per the SESLHD Records Management Standard.

A Risk Assessment can be found on the SESLHD intranet in the Support & Corporate Services page, Health ICT page then Processes.

5. DEFINITIONS

Amazon Web Services: a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

Azure: a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centres.

Certificate Management: the process of managing digital security certificates. This includes processes such as: Creation.

Cryptographic Key: a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication.

ICT System: a set-up consisting of hardware, software, data and the people who use them. It commonly includes communications technology, such as the Internet.

ICT and computers are not the same thing. Computers are the hardware that is often part of an ICT system.

Middleware: software that acts as a bridge between an operating system or database and applications, especially on a network.

Out of the Box: used to refer to the immediate usability or functionality of a newly purchased product, typically an electronic device or a piece of software.

Security Risk Assessment (SRA): a process of identifying, analysing and understanding information assets, possible impact of security risks, weaknesses and threats in order to apply appropriate security measures.

6. DOCUMENTATION

Procedural documentation for the management of systems accreditation is described in the Systems Accreditation Procedure.

7. REFERENCE DOCUMENTS

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

- SESLHD Information Security Policy SESLHDPD/310
- NSW Government Cyber Security Policy
- NSW Ministry of Health Policy Directive PD2013_033 - Electronic Information Security Policy

7.1 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 31000 Risk management - Principles and guidelines

8. REVISION AND APPROVAL HISTORY

Date	Revision	Author	Approval
March 2019	DRAFT	Initial draft. Shane Feeney Program Manager ICT Security & Strategy	Flora Karanfilovski Director, Health ICT
May 2019	DRAFT	Draft for comment period. No feedback received. Final version approved by Executive Sponsor. Formatted by Executive Services prior to tabling at June 2019 Executive Council Meeting.	Flora Karanfilovski Director, Health ICT
June 2019	1	Endorsed at June 2019 Executive Council meeting.	