

<b>NAME OF DOCUMENT</b>	ICT Systems Accreditation
<b>TYPE OF DOCUMENT</b>	Policy
<b>DOCUMENT NUMBER</b>	ISLHD CORP PD 57
<b>DATE OF PUBLICATION</b>	August 2019
<b>RISK RATING</b>	Low
<b>REVIEW DATE</b>	August 2024
<b>FORMER REFERENCE(S)</b>	
<b>EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR</b>	ISLHD Chief Information Officer
<b>AUTHOR</b>	Program Manager ICT Security & Strategy
<b>KEY TERMS</b>	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance.
<b>FUNCTIONAL GROUP OR HUB</b>	District Wide
<b>NSQHS STANDARD</b>	Standard 1
<b>SUMMARY</b>	This document provides the overarching policy which information systems should be accredited for use at Illawarra-Shoalhaven Local Health District.

**COMPLIANCE WITH THIS DOCUMENT IS MANDATORY**

This document is the intellectual property of Illawarra Shoalhaven Local Health District. Content cannot be duplicated without permission.

Feedback about this document can be sent to: [ISLHD-CorporateGovernance@health.nsw.gov.au](mailto:ISLHD-CorporateGovernance@health.nsw.gov.au)

## 1. POLICY STATEMENT

The security of Illawarra-Shoalhaven Local Health District (ISLHD) information is critical to meeting our information security obligations and to ensure the resilience and ongoing success of ISLHD.

The Systems Accreditation Policy addresses the risk the ISLHD infrastructure is exposed to when a new system is connected to the ISLHD 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 practice environment.

## 2. AIMS

The purpose of the Systems Accreditation (SA) Policy is to describe the principles used to manage and protect ISLHD 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 6 - 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. INFORMATION SECURITY POLICY SCOPE

A system is a regularly interacting or interdependent group of items, forming a unified whole, 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.

---

## ICT Systems Accreditation

## ISLHD CORP PD 57

---

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) or via [SARA](#). The system accreditation procedure can be found on the ISLHD 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). A SRA is conducted by Health ICT who can be engaged by lodging a request via [SARA](#).

### 4.4 Security Technology

If the system is using any security technology component (e.g. security token, authenticator, 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.

## 5. EXEMPTIONS

Any exemptions to the ICT 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 ISLHD Records Management Standard.

A [Risk Assessment](#) can be found on the ISLHD intranet in the Support & Corporate Services page, Health ICT page then Processes.

## 6. DEFINITIONS

### **Authenticator**

A mobile push authenticator is essentially a native app running on the claimant's mobile phone. The app uses public-key cryptography to respond to push notifications. In other words, a mobile push authenticator is a single-factor cryptographic software authenticator.

### **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.

### **Security Token**

A security token is a portable device that authenticates a person's identity electronically by storing some sort of personal information. The owner plugs the security token into a system to grant access to a network service. Security Token Services (STS) issue security tokens that authenticate the person's identity

## 7. DOCUMENTATION

The following documents may assist in providing guidance in accrediting new or rebuilt systems that are going to be installed on the district's digital infrastructure.

- [Systems Accreditation Procedure](#)
- [Risk Assessment Template](#)

## 8. AUDIT

The NSW Government has mandated via the [NSW Government Cyber Security Policy](#) that audits are to be conducted annually and the outcomes of the audit be reported to the district CIO where a risk assessment can be conducted on the non-compliances to determine the mitigation actions.

## 9. REFERENCE DOCUMENTS

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

- [ISLHD CORP PD 38 - Information Security Policy](#)
- [NSW Government Cyber Security Policy](#)
- [NSW Ministry of Health Policy Directive PD2013\\_033 - Electronic Information Security Policy](#)

### 9.1 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

**10. REVISION AND APPROVAL HISTORY**

Date	Revision	Author	Approval
March 2019	0	Program Manager ICT Security & Strategy	ISLHD Chief Information Officer
August 2019	0	Program Manager ICT Security & Strategy	Approval/Date: Corporate Policy recommendation Committee – August 2019
August 2019	0	Program Manager ICT Security & Strategy	Approval/Date: ISLHD Chief Information Officer – August 2019