INTERNAL ONLY

ISLHD POLICY COVER SHEET

NAME OF DOCUMENT	Service Continuity Policy for ICT Service Owners
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	ISLHD CORP PD 42
DATE OF PUBLICATION	April 2021
RISK RATING	Low
REVIEW DATE	April 2026
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Chief Information Officer
AUTHOR	Cyber Security Project Manager
KEY TERMS	ICT, Service Continuity, Business Continuity, Availability Management, Recovery, Incident, Crisis, Security, Disaster Recovery, Backup
FUNCTIONAL GROUP OR HUB	District wide
SUMMARY	This policy provides a framework for the process to prevent, predict and manage Information and Communications Technology (ICT) disruption and incidents, which have the potential to disrupt ICT services.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

Feedback about this document can be sent to: ISLHD-CorporateGovernance@health.nsw.gov.au

Service Continuity Policy for ICT Service Owners

ISLHD CORP PD 42

1. 1. DEFINITIONS

1.1. Information and Communications Technology (ICT)

Information and Communications Technology (ICT) includes all clinical and corporate applications and infrastructure supporting the operation of ISLHD.

1.2. Service Continuity

Service Continuity is a systematic process to prevent, predict and manage disruption and incidents which have the potential to disrupt ICT services. The process should result in a more resilient ICT service capability and less risk of interruption.

Service continuity involves:

- **Availability Management and Continuity Planning** practices to keep essential business processes and the supporting IT infrastructure running despite incidents and (limited) disasters including:
    - **Business Continuity Planning (BCP)** to ensure that critical business processes continue to operate satisfactorily despite a wide range of incidents.
    - **Continuity Planning (ITCP)** to ensure that ICT systems, networks and associated infrastructure and processes supporting critical business processes remain in operation despite disasters.
- **Recovery and Resumption Planning practices** for recovering or resuming business and ICT operations following incidents and disasters including:
    - **Business Resumption Planning (BRP)** to resume or restore critical and important business processes to something approaching normality following disasters or major incident that overwhelm the resilience capabilities.
    - **Disaster Recovery Planning (DRP)** for the recovery of critical ICT systems and services following a disaster that overwhelms the resilience arrangements.
    - **Incident Management (IM)** to evaluate and respond to information security-related incidents.
    - **Crisis Management (CM)** for the management of major incidents and crises, primarily relating to health and safety aspects.

1.3. Disaster Recovery

The term 'disaster recovery' refers to the process of recovering an information system from an incident or disaster to ensure service continuity.

1.4. Disaster Recovery Plan

The term 'Disaster Recovery Plan', also referred to as 'DRP', is the plan for managers of ICT services to determine how information systems can be recovered, in the event of a disaster. This plan minimises the risk of loss of service continuity.

1.5. ICT Service Owner

An ICT *Service Owner* is the person who has the primary responsibility to ensure that the ICT service delivers what it promises to consumers of the service. *Service Owners* may be external companies or may be LHD departments or services other than Health ICT.

1.6. Service Sponsor

The *Service Sponsor* is the individual responsible for signing off on, and accepting delivery of, a service. The *Service Sponsor* has the authority to accept service levels, costs, and risks associated with a service.

The *Service Sponsor* acts under their own authority or the authority of a Committee, group or executive-level position responsible for providing funding and/or resources to deliver the service and setting the strategic direction of the required service.

The *Service Sponsor* has the following responsibilities:

- Sets the strategic direction of the service
- Approves any changes to the service
- Determines and approves the agreed core business hours for the delivery of the service
- Provides communication to internal staff in respect of any changes and outage of the service
- Provides funding and/or resources to deliver service
- Signs off on and accepts delivery of a service

1.7. Senior Information Risk Officer

The *Senior Information Risk Officer* (SIRO) is an Executive Director or District Executive Team Member who will take overall ownership of the organisation's

information risk policies, acts as champion for information risk on the District Executive Team and provide written advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control regarding information risk. At ISLHD the SIOR is the Chief Information Officer.

1.8. Solution and Security Architect

The *Solution and Security Architect* is a Health ICT appointee reporting to the CIO. The role provides leadership and steering with respect to framework and approach for the strategic and technical design and planning of ICT infrastructures and security apparatus. The *Solution and Security Architect* is also the "design authority" for new services and solutions from the Health ICT and will authorise solutions before build work commences.

1.9. Senior Information Security Officer

The *Solution and Security Architect* is the *Senior Information Security Officer* (as referred to in relevant International Standards Organisation standards) for Illawarra Shoalhaven LHD, South Eastern Sydney LHD and Sydney Children's Hospital – Randwick.

2. POLICY STATEMENT

2.1. Purpose

The purpose of this *Service Continuity Policy* is to reduce the risk of interruption to ICT services and ensure that the organisation operates on a continuous basis.

2.2. Scope

All ICT services at Illawarra Shoalhaven Local Health District (ISLHD) including those managed by departments other than Health ICT. The current list of ICT services and their *Service Owners* is held by the Health ICT *Manager, Service Management.*

2.3. Service Continuity Planning

A Service Continuity (SCP) plan must be maintained and executed. The SCP may make use of any combination of recovery and/or restoration strategies including; hot, warm, cold standby data centres or servers; high-availability services within the same or across multiple data centres; services may be active/active or active/passive; it may utilize a ship-on-demand, shared services or cloud services, or any other approach.

A Disaster Recovery Plan (DRP) must be maintained and executed to ensure that ICT services can be recovered in the event of a disaster. The DRP must be updated at least annually and tested.

A Backup Plan must be maintained and executed to ensure that all files and applications are backed up on a regular basis. The Backup Plan must be updated at least annually and tested.

An Incident Management process must be implemented and maintained to respond to information security and other incidents.

3. TARGET AUDIENCE

This policy applies to all employees, contractors and other persons who, in the course of their work, design, manage and maintain ICT systems (*Service Owners*).

The policy applies to:

- NSW Health organisations
- non-government organisations receiving funding from ISLHD where compliance is included in the terms of their funding agreement
- private hospitals and day procedures centres treating public patients/clients on a contractual basis, where the contract includes requirements for compliance with NSW Health policies
- personnel of Health Professional Registration Boards
- Suppliers of services to ISLHD

Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for management, personnel and all persons handling information, whether directly or indirectly involved in client service delivery.

All personnel and organisations referred to above should be aware of their obligations and that the breach of those obligations may result in prosecution and the imposition of a penalty or disciplinary actions.

4. RESPONSIBILITIES

4.1. Chief Information Officer (CIO)

The CIO is the *Senior Information Risk Owner (SIRO)*, is responsible for information risk within the Local Health District and advises the District Executive Team on the effectiveness of information risk management across the organisation. The *Solution and Security Architect* has also been appointed as *Deputy SIRO* to support the *SIRO*.

External providers of information processing services must have their own *Senior Information Risk Officer*.

4.2. Senior Managers

Senior Managers are individually responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the policies, procedures and user obligations applicable to their area of work;
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities;

5. DOCUMENTATION

5.1. *Distribution Plan*

This document will be made available to all Staff via the LHDs' intranet sites.

A global notice will be sent to all Staff notifying them of the release of this document.

A link to this document will be provided from the Health ICT intranet site.

5.2. *Relevant Procedures*

Service Sponsors should satisfy themselves that *Service Owners* have appropriate procedures and plans in place to support this policy.

6. REFERENCES

- *NSW Government and Labelling Guidelines Version 2.0 Aug 2020*
- *Health Records and Information Privacy Act 2002 (HRIP Act)*
- *Privacy and Personal Information Protection Act 1998 (PPIP Act)*
- PD2009_076 *Communications - Use and Management of Misuse of NSW Health Communications Systems*
- PD2020_046 *Electronic Information Security – NSW Health*
- DCS-2020-02 *NSW Cyber Security Policy*
- *Broadcasting Services Amendment (Online Services) Bill 1999*
- PD2012_047 *Notifiable Conditions Data Security and Confidentiality*
- *NSW Health Privacy Manual for Health Information*
- AS ISO/IEC 27001:2015 *Information technology – Security techniques – Information security management systems – Requirements*
- AS ISO/IEC 27002:2015 *Information technology - Security techniques - Code of practice for information security controls*

- AS/NZS ISO/IEC 20000 *Information technology - Service management*
- State Archives and Records General Retention and Disposal Authority – Health Services, Public: Patient/Client records (GDA17)
- State Records General Retention and Disposal Authority – Imaged Records (GA36)
- Australian Standard AS2828.2:2019 Health Records Part 2 Digitized (scanned) health records system requirements.

7. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
7/7/2015	0	Maggie Alexander, Draft for initial consultation
13/7/2015	0.1	André Snoxall, CIO, Update for consultation
17/7/2015	0.2	André Snoxall, CIO, Update after discussion in Health ICT
20/7/2015	0.3	Jon Straker, Acting Group Manager Architecture and Security
April 2021	1.0	Cyber Security Project Manager **Approval/Date:** Corporate Policy Recommendation committee/ March 2021 **Approval/Date:** Chief Information Officer/ April 2021