SESLHD POLICY COVER SHEET

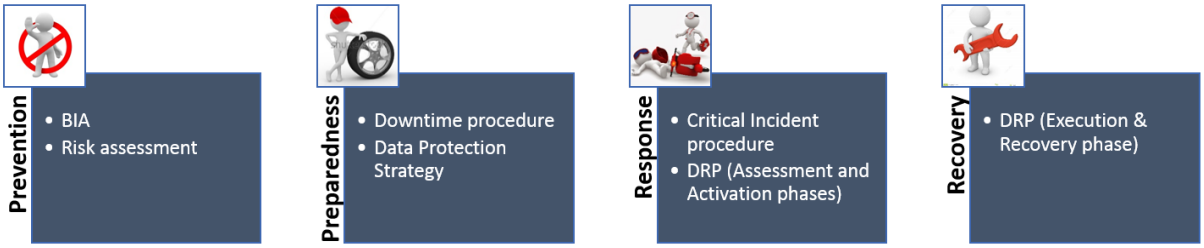
Health
South Eastern Sydney
Local Health District

NAME OF DOCUMENT	Service Continuity Policy for Health ICT Services
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/288
DATE OF PUBLICATION	August 2021
RISK RATING	High
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Standard 1- Clinical Governance
REVIEW DATE	August 2023
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Andrew Elliott | Head Health ICT Anne Milne | Director, Corporate and Legal Services
AUTHOR	Ayman Essmat Ayman.essmat@health.nsw.gov.au
POSITION RESPONSIBLE FOR THE DOCUMENT	Health ICT Service Manager Ayman Essmat Ayman.essmat@health.nsw.gov.au
FUNCTIONAL GROUP(S)	Health ICT
KEY TERMS	
SUMMARY	This policy provides consistent, transparent and accountable governance framework to improve alignment of ICT service continuity management with SES clinical and non-clinical functions that have critical ICT dependencies

Feedback about this document can be sent to SESLHD-Policy@health.nsw.gov.au

1. POLICY STATEMENT

The comprehensive approach to emergency or disaster management incorporates the key components of Prevention, Preparedness, Response and Recovery.



Prevention statements:

A *Business Continuity Plan (BCP)* must be maintained and executed. The BCP 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 utilise a ship-on-demand, shared services or cloud services, or any other approach.

Preparedness statements:

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 and tested at least annually.

Response statement

A *Critical Incident Management* process must be implemented and maintained to respond to information security and other incidents.

Recovery statement:

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 and tested on a regular basis.

2. AIMS

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

3. TARGET AUDIENCE

The 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 SESLHD 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 SESLHD

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

Head of ICT

The Head Health ICT (CIO / Director ICT) 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. External providers of information processing services must have their own Senior Information Risk Officer.

Senior ICT 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. DEFINITIONS

Business Continuity Plan (BCP): a plan defining the steps required to restore business processes following a disruption. The plan also identifies the triggers for invocation, people to be involved, communications etc. IT service continuity plans form a significant part of business continuity plans.

ICT Service Continuity Plan: a plan defining the steps required to recover one or more IT services. The plan also identifies the triggers for

invocation, people to be involved, communications etc. The IT service continuity plan should be part of a business continuity plan.

Disaster Recovery Plan (DR): a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, so an organization will continue to operate – or quickly resume key operations.

Downtime procedure: defined procedures and guidelines that will be followed by business users when the IT services is inaccessible or completely down.

Critical incident procedure: procedure to detail the timely response to emergencies and critical incidents and reduce the impact of such incidents through the appropriate use of resources.

6. DOCUMENTATION

- NSW Ministry of Health Policy Directive PD2020_046 - Electronic Information Security Policy
- NSW Ministry of Health Policy Directive PD2015_043 - Risk Management - Enterprise-Wide Risk Management Policy and Framework
- NSW Government Disaster Recovery Guidelines
- Health ICT Disaster Recovery Plan
- Health ICT Information Security Policy
- NSW Government Information Classification and Labelling Guidelines
- Health ICT Critical Incident procedure
- Service Catalogue

7. REFERENCES

NSW Ministry of Health Policy Directive PD2015_043 - Risk Management - Enterprise-Wide Risk Management Policy and Framework
NSW Ministry of Health Policy Directive PD2020_046 - Electronic Information Security Policy
NSW Government Disaster Recovery Guidelines
Health ICT Disaster Recovery Plan
Health ICT Information Security Policy
NSW Government Information Classification and Labelling Guidelines
Health ICT Critical Incident procedure
Health ICT Business Continuity Plan v1.0

8. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval

7/7/2015	0	Maggie Alexander, Draft for initial consultation
13/7/2015	1	André Snoxall, CIO, Update for consultation
17/7/2015	2	André Snoxall, CIO, Update after discussion in IMSD
20/7/2015	3	Jon Straker, Acting Group Manager Architecture and Security
October 15	3	Endorsed for Draft for Comment
November 2015	3	No Feedback received. Proceed to DET for approval.
10 December 2015	3	Endorsed by DET.
28/8/2018	4	Ayman Essmat , ICT Service Manager
August 2018	4	Flora Karanfilovski, Director Health ICT
July 2021	5	Minor review: Service continuity approach diagram added to Policy Statement; Definitions Updated. Endorsed by Head of Health ICT and Executive Sponsor.