SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	Service Continuity Policy for Health ICT Services
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/288
DATE OF PUBLICATION	August 2018
RISK RATING	High
LEVEL OF EVIDENCE	1. Health records management systems support the collection of information and meet the consumer/patient and organisation's needs. 2. Corporate records management systems support the collection of information and meet the organisation's needs.
REVIEW DATE	August 2020
FORMER REFERENCE(S)	
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Flora Karanfilovski Director ICT
AUTHOR	Ayman Essmat ICT Service Manager
POSITION RESPONSIBLE FOR THE DOCUMENT	Ayman Essmat ICT Service Manager
KEY TERMS	
SUMMARY *Brief summary of the contents of the document*	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.

Service Continuity Policy for Health ICT Services

SESLHDPD/288

1. SCOPE

All ICT services at South Eastern Sydney Local Health District (SESLHD) including those managed by department's other than Health ICT. The current list of ICT services and their Service Owners is held by the ICT Service Manager.

2. POLICY STATEMENT

2.1. 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.

2.2. 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.

2.3. 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.

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

3. 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.

4. 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.

5. RESPONSIBILITIES

5.1. Director ICT

The 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.

5.2. 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.

6. DEFINITIONS

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.
  - ICT 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:
  - Disaster Recovery Planning (DRP) for the recovery of critical ICT systems and services following a disaster that overwhelms the resilience arrangements.
  - Critical Incident Management (IM) to evaluate and respond to information security related incidents.

7. DOCUMENTATION

Health ICT Business Continuity Plan
Health ICT Disaster Recovery Plan
Health ICT DRP Communication Plan
Health ICT DRP Training Plan
Health ICT Critical Incident Procedure

8. REFERENCES

Risk Management - Enterprise-Wide Risk Management Policy and Framework – NSW Health
NSW Government Disaster Recovery Guidelines
Electronic Information Security Policy - NSW Health PD2013_033
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

9. 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