SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	Digital Asset Management
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/322
DATE OF PUBLICATION	March 2025
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Standard 1 – Clinical Governance
REVIEW DATE	March 2030
FORMER REFERENCE(S)	Nil
EXECUTIVE SPONSOR	Director, Digital Health (ICT)
AUTHOR	Shane Feeney
POSITION RESPONSIBLE FOR THIS DOCUMENT	Jith Perera Head, Business Technology Services jith.perera@health.nsw.gov.au
FUNCTIONAL GROUP(S)	Information Management and Data
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, asset management.
SUMMARY	The document provides the overarching policy under which digital information assets are managed throughout their lifecycle in South Eastern Sydney Local Health District.

1.   POLICY STATEMENT

The purpose of the Digital Asset Management Policy is to provide the framework for the management of ICT equipment from acquisition to disposal. The policy also provides the principles used to manage and protect SESLHD digital assets.

This policy draws from the NSW Government Financial Regulations and SESLHD Policy Directive SESLHPD/310 - Information Security.

Digital asset management differs to the standard practice of procurement asset management, as digital asset management provides a mechanism to aid the support and management throughout the lifecycle of the asset, such as ensuring the asset has a service level agreement (SLA).

Digital assets can be a service such as the eMR, which consists of several physical servers, has a configuration, and connects to other systems.

Appropriate actions must be taken to protect digital assets against physical or financial loss whether by theft, miss-handling or accidental damage, either through primary prevention (e.g. physical security), or remediation (e.g. marking) and ensuring the asset has the appropriate contracts and support staff skills.

Information about digital assets shall be held in a suitable electronic database that enables them to be tracked, managed and audited throughout the entire lifecycle.

2.   AIMS

Digital assets hold and manipulate information, therefore it is important that all digital assets, whether software or hardware, are appropriately managed from acquisition to time of disposal. This ensures that the asset delivers best value for money and appropriately protects the information that passes through them.

3.   DIGITAL ASSET MANAGEMENT POLICY SCOPE

This policy applies to all digital assets managed by either Digital Health or Specialist ICT (SICT), or others who purchase a digital asset whether paid by SESLHD or otherwise. A digital asset is defined as:

- desktop, laptop and server computers and associated infrastructure

- monitors, printers and scanners

- phones, mobile and smartphones and portable computing equipment

- routers, firewalls, switches, access points and other network infrastructure

- software applications and their licenses

- any other ICT digital peripheral equipment not of a disposable nature. As ICT is by nature constantly changing, other items not listed here may still be required to be included in the asset management policy, or associated processes.

- internet of things devices – which are embedded with electronics, internet connectivity, and other forms of hardware, such as sensors. These devices can communicate and interact with others over the internet, and can be remotely monitored and controlled. Refer to SESLHD Policy Directive - SESLHDPD/312 Internet of Things (IoT) for further information

- medical digital instruments or devices that are <u>not</u> part of an accreditation inventory, for

example, required by either FDA, TGA or EMDA that require specialist asset tracking

- staff specialists purchasing hardware or devices such as mobile phones, or tablets from SP&T or TESL funds (for level one staff specialists) and number two trust accounts (for level two to five staff specialists) are to purchase items from the advertised devices and equipment on SESLHD's HICT Procurement page.

The device/hardware is to be configured like a standard corporate device meeting licencing, software and anti-virus security requirements aligning with SESLHD Policy Directive - SESLHDPD/310 Information Security Policy. All assets are tagged and remain the property of the LHD.

To configure the device to meet security governance and compliance guidelines, a request is to be logged by the owner in eHealth's ticketing portal SARA. HICT will configure the device/hardware to meet the directive.

3.1　Digital Asset Management Registration

Departments must register digital assets that require ongoing maintenance and support or creates a potential risk in terms of financial loss, data loss or exposure which must be documented and controlled to meet LHD digital asset management requirements.

The recorded information must be sufficient information that will sustain support and lifecycle management functions.

3.2　Digital Asset Management Repository

Digital Health hosts the Configuration Management Database (CMDB) which is the designated repository. Agencies need an inventory and/or access to an inventory of the IT hardware assets used to support their mission and automated solutions. An agency and/or its service provider must know what IT hardware assets they have and where those assets are located in order to protect them.

When determining what information to track for a particular asset, consider the following:

1. specific information pertinent to the particular hardware asset
2. physical location
3. unique identifier of the asset
4. support contract and information

Appendix A contains the Example and Template IT Hardware Asset Inventory and the Template for registering the Application (Software) Asset.

Agencies and/or service providers should address labeling IT hardware assets. Labeled assets assist when troubleshooting problems, tracking and identifying inventory, and recovering lost or stolen IT hardware assets such as laptops and personal digital assistants (PDA's).

Appendix B contains the Example and Template IT Hardware Asset Label. When an IT hardware asset is being moved or transferred from one location, or responsible party to another, both parties should sign a log indicating acknowledgement of the transfer.

4.　　RESPONSIBILITY

Director, Digital Health

The Director Digital Health is accountable for the implementation of this policy. Responsibility of the day-to-day operation is normally delegated to the Digital Health Managers.

Digital, Health Managers

All Health ICT Managers have responsibility for (delegating where appropriate):

- coordinating the audit of the equipment their team supports
- updating and maintaining the accuracy of the inventory, such as equipment moves
- ensuring that equipment is signed for, without amendment, by equipment holders and declaration is scanned into the asset management system
- applying ICT supplied barcode asset tag before equipment is taken out of ICT Services care
- checking equipment is returned in the same configuration as expected and signing pro-forma receipts upon collection from equipment holders
- care of ICT equipment held in stock for issuing and awaiting transfer for disposal
- provide reports on any assets stripped for spares to the departmental manager and Health ICT Senior Information Officer (SISO) and note components removed within the asset management system. Data on harvested drives will immediately have data destructed using a method approved by the SISO or delegate
- printing and issuing replacement asset and location bar codes
- recording the digital asset information, hardware or software, in the Health ICT Configuration Management Database (CMDB) using the CMDB portal to enter the data.

Digital Health, Head Business Technology Services

The Digital Health Head Business Technology Services has responsibility for (and delegating where appropriate):

- ensuring that on collection new equipment is signed for by IT staff. IT equipment will not be issued by the purchasing team to porters or end users
- issuing and fixing asset tags for IT equipment purchased through IT Services
- entering purchasing information on the asset management system
- care for and security of equipment once transferred from technical and support teams for disposal
- creating an asset list prior to disposal agents collection
- confirming asset disposal on system using disposal reports
- marking equipment as lost or stolen from the asset register (CMDB)
- creating management reports including the annual audit report for the Director of Finance
- adding ICT equipment to the CMDB that was not purchased through Digital Health

- ensuring the correct adherence to this policy by Digital Health team members at all times.

Heads of Department and Directors of Departments

Staff who have been issued ICT equipment have the following responsibilities for the equipment in their care:

- loss or theft of ICT equipment must be reported immediately to the SISO and Digital Health Head Business Technology Services

- all ICT equipment, including LHD issued equipment, must be returned to the relevant ICT support team upon replacement, equipment redundancy (i.e. no longer required for business) or when the holder severs affiliation. Equipment holders will retain responsibility for equipment issued to them until it has been returned to Digital Health or the Department for redeployment or disposal

- equipment holders are not permitted to transfer their responsibilities to another staff member without the joint consent of the asset holder. Fixed IT equipment must not be moved without the consultation of the department head and/or Digital Health and an update of asset data must be made

- equipment holders must present mobile assets such as laptops and mobile phones to their support team for auditing within two weeks of request. Equipment may be presented for auditing at any time, but all equipment must be accounted for within a year of issuing or last being audited

- ICT equipment holders must make every effort to ensure that the equipment barcode asset marking is not damaged or destroyed whilst in their care

- in the event that a bar code asset marking has been damaged or destroyed, the equipment holder must contact the appropriate support team immediately to arrange for a replacement marking

- return equipment immediately that is not operating normally to their support team.

Staff and Representatives of Digital Health

All Digital Health staff and associated representatives must also ensure that they follow this policy, including:

- ensuring that any ICT asset that is retired is disposed of in the correct way

- updating asset registers correctly and as soon as a change is made

- provide correct and appropriate advice to users on the correct handling of IT assets

- that any incorrect disposal or misuse of an IT asset is reported to an appropriate manager within either Digital Health or the department head as soon as possible.

5.   DEFINITIONS

Abbreviation	Definition
CIO	Chief Information Officer
CMDB	Configuration Management Database
EMDA	European Medial Device Authority
eMR	Electronic Medical Records
FDA	U.S Food and Drug Administration
HICT	Health Information Communications Technology
ICT	Information Communications Technology
IoT	Internet of Things
LHD	Local Health District
SARA	Search And Request Anything (eHealth Service)
SESLHD	South Eastern Sydney Local Health District
SICT	Specialist Information Communications Technology
SLA	Service Level Agreement
TGA	Therapeutic Goods Association

6.   REFERENCE DOCUMENTS

The following documents are referenced in this policy:

   a. **Legislation, Policies and Guidelines**
   - *Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)*
   - *Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)*
   - NSW Cyber Security Policy
   - NSW Government Classification Labelling and Handling Guidelines
   - NSW Government Procure IT Framework v3.2
   - NSW Health Policy Directive PD2020_046 - Electronic Information Security
   - SESLHD Policy Directive SESLHDPD/310 - Information Security Policy
   - SESLHD Policy Directive SESLHDPD/312 - Internet of Things (IoT)

   b.   **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

7.   VERSION AND APPROVAL HISTORY

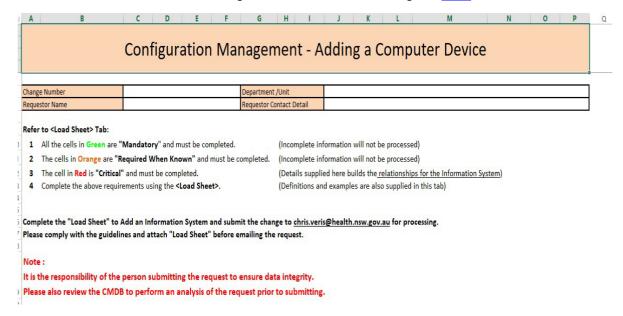| Date	Version No	Author and approval notes
09/01/2018	1.0	Shane Feeney, Program Manager ICT Security and Strategy. Approved by Flora Karanfilovski, Director - Health ICT
01/08/2019	1.1	Richelle Risi, Business Analyst Health ICT Operations. Approved by Flora Karanfilovski, Director - Health ICT
18/10/2019	Draft	Registered by Executive Services and posted on Draft for Comment.
29/01/2020	1.2	Feedback incorporated and final draft version approved by Flora Karanfilovski, Director - Health ICT.
February 2020	1.2	Processed by Executive Services prior to tabling at February 2020 Executive Council meeting.
April 2020	1.2	Approved at April 2020 Executive Council meeting. Published by Executive Services.
26 March 2025	1.3	Minor review, hyperlinks updated.

Appendix A

Health ICT Hardware Asset Registration

- Desktop and laptop registration is auto generated via active directory managed policies.

- Mobile devices are registered in a vendor managed database

- Heath ICT hosted servers are registered in the CMDB using the form below:

Configuration Management - Adding a Computer Device

Change Number		Department /Unit	
Requestor Name		Requestor Contact Detail	

Refer to <Load Sheet> Tab:

1. All the cells in **Green** are "**Mandatory**" and must be completed. (Incomplete information will not be processed)
2. The cells in **Orange** are "**Required When Known**" and must be completed. (Incomplete information will not be processed)
3. The cell in **Red** is "**Critical**" and must be completed. (Details supplied here builds the relationships for the Information System)
4. Complete the above requirements using the **<Load Sheet>**. (Definitions and examples are also supplied in this tab)

Complete the "Load Sheet" to Add an Information System and submit the change to chris.veris@health.nsw.gov.au for processing.
Please comply with the guidelines and attach "Load Sheet" before emailing the request.

Note :

It is the responsibility of the person submitting the request to ensure data integrity.
Please also review the CMDB to perform an analysis of the request prior to submitting.

Configuration Item	Input here ONLY	GUIDELINES	
		Definitions	**Examples**
Computer Register	**Computer Register**	**Computer Register**	**Computer Register**
Hostname	RANTQA01	Unique Host name	RANPAS01
FQDN hostname	ERC034.lan.sesahs.nsw.gov.au	FQDN of Host	RANPAS01.lan.sesahs.nsw.gov.au
Domain	lan.sesahs.nsw.gov.au	Domain Name	lan.sesahs.nsw.gov.au
Application Name	Cerner Millinium	This is Critical field: Application relationship mapping Note: this data element maps servers to new/existing applications (ie. Clinical, Corporate, Infrastructure) & is key for relationship mapping. **Enter: known relationships to applications in the "Application Register"**	eg. iPharmacy, Cerner Millinium, CORD, PathNet etc
Server Type (Physical/ Virtual)	Virtual	Is this Host Physical or Virtual	Physical or Virtual
IP address	10.45.214.60	IP Address of Ci. All IPS are entered	10.45.209.204 169.254.3.219 192.168.10.103 192.168.10.182
OS Version	Windows Server 2012 R2 Datacentre	Operating System running on the Host	Microsoft Windows Server 2012 R2 Datacenter
Hardware Vendor	VMware, Inc.	Hardware Vendor for Physical Server (otherwise refer example)	eg. Physical: Hewlett-Packard Virtual: VMware, Microsoft (for HyperV)
Hardware Model	VMware Virtual Platform	Hardware Model of Physical Server (otherwise refer example)	eg: Physical: HP ProLiant DL560 Gen8 Virtual: Virtual Machine (for HyperV)
Number of CPU cores (vCPUs in case of VMs)	2	Number of CPU cores	4
Memory size (GB)	7	Physical Memory Allocation (GB)	200
Location	Data Centre - Lawson House - Level 3 - Wollongong Hospital	Physical loctaion of Ci, if Virtual leave blank	Prince Of Wales Server Farm 2
Local Storage (GB)	299	Local physical storage (GB)	99
Subnet	10.45.212.0/22	Identifies Network addresses by dividing IP address into network and host address	10.45.208.0/22 169.254.0.0/16 192.168.10.0/24
Server Function	TQAS Application and Database server	Short Description of the Function of the Server	Citrix 6.5 Production (SESIFARM01) - Varian ARIA Med Onc Server

'Appendix A – Health ICT Hardware Asset form'

Digital Health - Software Asset Registration Form

An extract of the form and required criteria is displayed below:

Configuration Management - Add an Information System

Change Number		Department /Unit	
Requestor Name		Requestor Contact Detail	

Refer to <Load Sheet> Tab:

1　All the cells in **Green** are **"Mandatory"** and must be completed.　　(Incomplete information will not be processed)

2　The cells in **Orange** are **"Required When Known"** and must be completed.　(Incomplete information will not be processed)

3　The cell in **Red** is **"Critical"** and must be completed.　　(Details supplied here builds the relationships for the Information System)

4　Complete the above requirements using the **<Load Sheet>**.　　(Definitions and examples are also supplied in this tab)

Complete the "Load Sheet" to Add an Information System and submit the change to chris.veris@health.nsw.gov.au for processing.
Please comply with the guidelines and attach "Load Sheet" before emailing the request.

Note :
It is the responsibility of the person submitting the request to ensure data integrity.
Please also review the CMDB to perform an analysis of the request prior to submitting.

Configuration·Item¤	Input·here·ONLY¤	GUIDELINES¤	
		Definitions¤	**Examples¤**
Application·Register¤	**Application·Register¤**	**Application·Register¤**	**Application·Register¤**
Information·System¤	¤	Full·name·of·application·or·system·as·known·by·the·business¤	iPharmacy,·Age-Care·Evaluation,·Breast·Screening·Patient·Information·System¤
Description¤	¤	Description·of·the·System·--·Overview·of·the·function·and·services·it·provides¤	CBORD·--·Food·Services·Meal·and·Menu·Management·System·for·Kitchens,·dietary·management,·supplies·and·logistics·software¤
Computer¤	¤	Server·(Physical·or·Virtual)·supporting·the·Information·System¤	RANAPP01↵ RANARG03↵ RANARG10↵ RANARG11↵ RANEMR20↵ RANEMR21↵ RANPAS01¤
Category¤	¤	**Clinical·-**·services·refer·to·all·services·and·information·systems·that·directly·support·Clinical·processes·and/or·the·majority·of·the·their·end·user·are·clinical·staff·such·as·eMR,·iPM,·iPharmacy,·…↵ ↵ **Corporate·-**·Services·refer·to·all·services·and·information·systems·that·mainly·support·corporate·processes·and/or·the·majority·of·the·their·end·user·are·admin·staff·such·as·Video·Conference,·Web·content·Management,·Internet,·Desktop·Service,·Printing·service·…↵ ↵ **Infrastructure·-**·Services·refer·to·all·supported·services·that·required·to·enable·clinical·and·corporate·services·and/or·the·majority·of·the·their·end·user·are·IT·staff·such·as·Backup·service,·Citrix,·Data·Centre,·Active·Directory,·…¤	Clinical,·Corporate,·Infrastructure¤

'Appendix A – Health ICT Software Asset form'

Appendix B

'Appendix B - SESLHD Asset Tag example'