

INTERNAL ONLY
ISLHD POLICY
COVER SHEET



Health
 Illawarra Shoalhaven
 Local Health District

NAME OF DOCUMENT	ISLHD Digital Asset Management
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	ISLHD CORP PD 07
DATE OF PUBLICATION	April 2020
RISK RATING	Low
REVIEW DATE	April 2025
FORMER REFERENCE(S)	Nil
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Chief Information Officer – ISLHD Health ICT
AUTHOR	Business Analyst – Health ICT
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, Asset Management
FUNCTIONAL GROUP OR HUB	http://islhnweb/Policies_Procedures_Guidelines/default.asp
NSQHS STANDARD	Standard 1
SUMMARY	The document provides the overarching policy under which digital information assets are managed throughout their lifecycle in 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

1. POLICY STATEMENT

The purpose of the Asset Management policy provides the overall framework for the management of ICT equipment from acquisition to disposal. This policy draws from the NSW Government Financial Regulations and the LHD Information Security Policy. 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 that the asset has a service level agreement (SLA).

Digital assets can be a service such as the eMR system which consists of several physical servers and has a configuration and integration 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 ensure that 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. BACKGROUND

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 to ensure that the asset delivers best value for the investment and appropriately protects the information that passes through them.

The purpose of the Digital Asset Management Policy is to provide the principles used to manage and protect ISLHD digital assets.

Definitions

Abbreviation	Definition
CIO	Chief Information Officer
ISLHD	Illawarra Shoalhaven Local Health District
ICT	Information Communications Technology
LHD	Local Health District
SLA	Service Level Agreement
eMR	Electronic Medical Records
HICT	Health Information Communications Technology
SICT	Specialist Information Communications Technology

SARA	Search And Request Anything (eHealth Service)
IoT	Internet of Things
FDA	U.S Food and Drug Administration
TGA	Therapeutic Goods Association
EMDA	European Medical Device Authority
CMDB	Configuration Management Database
NAC	Network Access Control

3. RESPONSIBILITIES

3.1 The CIO – ISLHD will:

- Adhere to the content of this document.
- Is accountable for the implementation of this policy in the LHD and is responsible of the day-to-day operations which is normally delegated to the Health ICT Managers.

3.2 Health ICT Managers will:

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

- Adhere to the content of this document.
- 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.

3.3 Health ICT Operations Manager will:

Note: Health ICT Operations Manager has responsibility for (and delegating where appropriate):

- Adhere to the content of this document
- 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 agent's 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
- Upon discovery adding ICT equipment to the CMDB not purchased through Health ICT Services
- Ensuring the correct adherence to this policy by Health ICT team members.

3.4 Heads of Department and Directors of Departments will:

This includes employees and contingent workers who have been issued ICT equipment have the following responsibilities for the equipment in their care:

- Adhere to the content of this document.
- Loss or theft of ICT equipment must be reported immediately to the SISO and Health ICT Operation Manager.
- 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 Health ICT Services 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 Health ICT Services 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 2 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 where 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.
- Ensure staff are aware of, and adhere to, this document.

3.5 Staff and Representatives of Health ICT Services

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

- Adhering to the content of this document.
- 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 Health ICT or the department head as soon as possible.
- Ensure staff are provided with the training and equipment to perform this procedure.

4. POLICY

This policy applies to all Digital assets managed by either Health ICT (HICT), or Specialist ICT (SICT) or others who purchase a digital asset whether paid by ISLHD 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 they can be remotely monitored and controlled refer to the ISLHD Internet of Things (IoT) Policy for further information.
- Medical digital instruments or devices that are not part of an accreditation inventory, i.e.: Required by either FDA, TGA or EMDA that require specialist asset tracking.
- Staff Specialists purchasing hardware or devices (mobile phones, tablets) from SP&T or TESL funds (for Level 1 Staff Specialists) and Number 2 Trust Accounts (for level 2-5

Staff Specialists) are to purchase items from the advertised devices and equipment on the [Districts 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 the Districts 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 [SARA](#) eHealth's ticketing portal. HICT will configure the device/hardware to meet the directive.

Digital Asset Management Registration

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

The recorded information must be sufficient to support the lifecycle of the asset.

Digital Asset Management Repository

Health ICT 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 the location in order to protect them.

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

1. Specific information pertinent to the 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.

It is a recommendation of Health ICT that Agencies and/or service providers label all 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).

5. DOCUMENTATION

References include:

- 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

6. AUDIT

Audits are conducted when requested and are measured against the ISO27001 framework using the CIA – Confidentiality, Integrity and Availability principles. Evidence of records are maintained in Health ICTs [CMDB](#). Devices will not connect to the environment until they are registered on the NAC – Network Access Control where security controls are configured to proactively mitigate the risk of a security breach (es).

7 REFERENCES

The following documents are referenced in this policy:

Legislation, Policies and Guidelines.

- [ISLHD Information Security Policy](#)
- [NSW Government Digital Information Security Policy](#).
- [Electronic Information Security Policy – NSW Health](#)
- [NSW Government Classification Labelling and Handling Guidelines](#).
- [Privacy and Personal Information Protection Act 1998 \(NSW\) \(PIIP Act\)](#).
- [Health Records and Information Privacy Act 2002 \(NSW\) \(HRIP Act\)](#).
- [NSW Government Procure IT Framework v3.2](#)

8. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
April 2020	0	Business Analyst – Health ICT Approval/Date: Corporate Policy Recommendation committee / April 2020 Approval/Date: Chief Information Officer / April 2020

9. APPENDIX 1 –

Health ICT Hardware Asset Registration

- Desktop and Laptops registration is auto generated via Active Directory managed policies.
 - Mobile devices are registered in a Vendor managed database
- Health 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							
<p>Refer to <Load Sheet> Tab:</p> <p>1 All the cells in Green are "Mandatory" and must be completed. (Incomplete information will not be processed)</p> <p>2 The cells in Orange are "Required When Known" and must be completed. (Incomplete information will not be processed)</p> <p>3 The cell in Red is "Critical" and must be completed. (Details supplied here builds the relationships for the Information System)</p> <p>4 Complete the above requirements using the <Load Sheet>. (Definitions and examples are also supplied in this tab)</p> <p>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.</p> <p>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.</p>												

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	<p>This is Critical field:</p> <p>Application relationship mapping</p> <p>Note: this data element maps servers to new/existing applications (ie. Clinical, Corporate, Infrastructure) & is key for relationship mapping.</p> <p>Enter: known relationships to applications in the "Application Register"</p>	eg. iPharmacy, Cerner Millinium, COD, 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 location 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'

Health ICT - 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:

- All the cells in **Green** are "Mandatory" and must be completed. (Incomplete information will not be processed)
- The cells in **Orange** are "Required When Known" and must be completed. (Incomplete information will not be processed)
- The cell in **Red** is "Critical" and must be completed. (Details supplied here builds the relationships for the Information System)
- 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 CMDR 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		<p>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, ...</p> <p>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, ...</p> <p>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, ...</p>	Clinical, Corporate, Infrastructure

Appendix A – Health ICT Software Asset form