INTERNAL ONLY

ISLHD POLICY COVER SHEET

NAME OF DOCUMENT	Information Security Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	ISLHD CORP PD 38
DATE OF PUBLICATION	August 2018
RISK RATING	Low
REVIEW DATE	August 2023
FORMER REFERENCE(S)	ISLHD OPS PD 38
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Executive Director Corporate Services, Assets and Chief Information Officer
AUTHOR	Program Manager, ICT Security & Strategy Health ICT
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance
FUNCTIONAL GROUP OR HUB	District-wide
NSQHS STANDARD	Standard 1
SUMMARY	This document provides the overarching policy under which information should be handled at Illawarra-Shoalhaven Local Health District

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

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

Health
Illawarra Shoalhaven
Local Health District

Information Security ISLHD CORP PD 38

1. POLICY STATEMENT

The Information Security Management Systems (IS) policy recognises that ownership of records of the care provided to a patient (Personal-Health-Information) and information on supporting systems is often a contentious issue and that, as stewards of this private and confidential information, ISLHD has a primary responsibility to ensure that they maintain the security and integrity of the data.

ISLHD also has a responsibility to ensure that Personal-Health-Information records are used in a way that are used in a way that a patient would reasonably expect to be necessary to support their care.

The policy further recognises that broad clinical access to patient records is necessary to the safe and effective functioning of an evidence-based integrated healthcare system.

ISLHD has a duty of care and legislative requirement to their staff and the community at large and there will be occasions when confidential and sensitive information must be shared to meet this duty of care; in these circumstances the policy ensures that appropriate controls, review and audit is in place to be able to monitor and manage information access.

2. AIMS

The purpose of the Information Security Policy is to describe the principles used to manage and protect ISLHD digital assets. Information Security applies to and is delivered through People, Process and Technology. The tripartite of People, Processes and Technology has a responsibility to ensure that the security of information within ISLHD maintains Confidentially, Integrity and Availability (CIA) to the minimum standards required.

Information Security mandated standards are set out in the NSW Government Digital Information Security Policy which specifies the use of ISO27001 as the framework and minimum information security controls to deliver secure systems. Information security is managed and conveyed through a framework called Information Security Management System (ISMS).

The purpose of the Information Security Policy is to provide the principles that are to be used to govern, manage and protect ISLHD digital assets and is the key policy of the Information Security Management System (ISMS)

The Information Security Policy specifies principles which ISLHD must;

a) Examine the organisation's information security risks, taking account of internal and external threats, systems vulnerabilities, and probable impacts to ISLHD;

b) Implement an information security design which will produce a coherent and comprehensive suite of information security controls and/or forms of risk treatments (such as risk avoidance or risk transfer) to address risks that are deemed unacceptable and;

c) Adopt a governance that is to guide information security polices, process and controls to meet the LHD's information security needs on an ongoing basis.

It is the responsibility of Departmental/ Business Owners or Managers of digital assets to ensure compliance with this policy.

The Information Security Policy is a primary policy supported by several technical information security policies and should not be considered in isolation but together and shall have equal standing.

The following diagram, Figure 1. ISMS Policy Context shows the library of polices in relation to the IS and supporting technical policies.

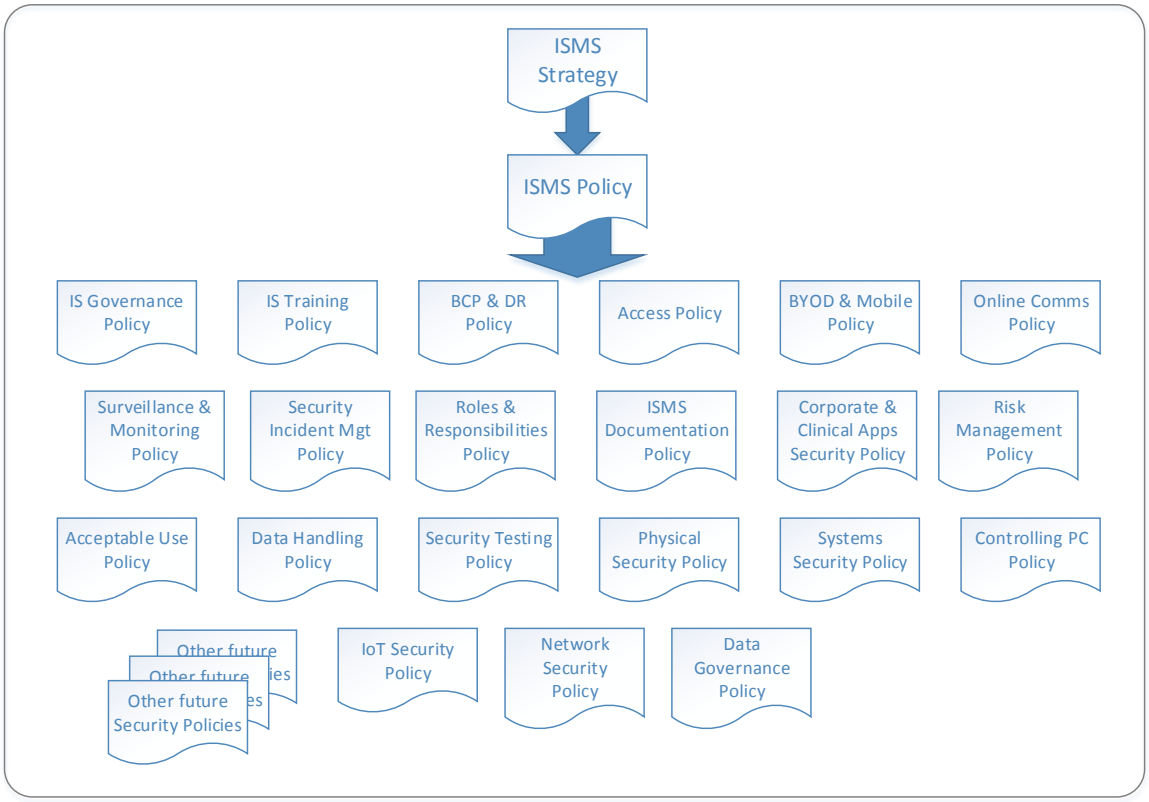

Figure 1. ISMS Policy Context

2.1 Policy Scope

This Policy applies to all staff who interact, manage or have responsibility over digital assets and information held electronically including photographs, video recordings, film, recorded sound and images. No distinction is made as to the type of medium on which the information is stored as the policy is intended to be technology independent.

Where ambiguity exists regarding the use of, or access to information, an initial consultation with the ISLHD Information Security Governance Committee (ISGC) must occur who will give guidance and interpret the information security controls to assist and mitigate an adverse impact on the care or business operations.

The ISMS is a framework that is a collection of policies, processes and other documents that consists of the following;

a) Business, ICT and ISMS strategies;
b) Security Governance;
c) Policies covering all aspects of information security;
d) Processes and procedures that have an information security component;
e) Controls and standards;
f) Metrics and measurements;
g) Roles and responsibilities;
h) Risk Management;
i) Continuous improvement program.

The diagram in Figure 2. Information Security Management System architecture – IS shows the context of the ISMS Framework and the interrelationships between each of the artefacts. This document is the prime policy which supports the governance of information security and dictates the principles upon which Information Security is to be managed.

The IS Policy is supported by several technical policies that are topic specific to allow for portability and adaptability as the environment changes and new requirements emerge and old ones are retired as part of the continuous improvement program.

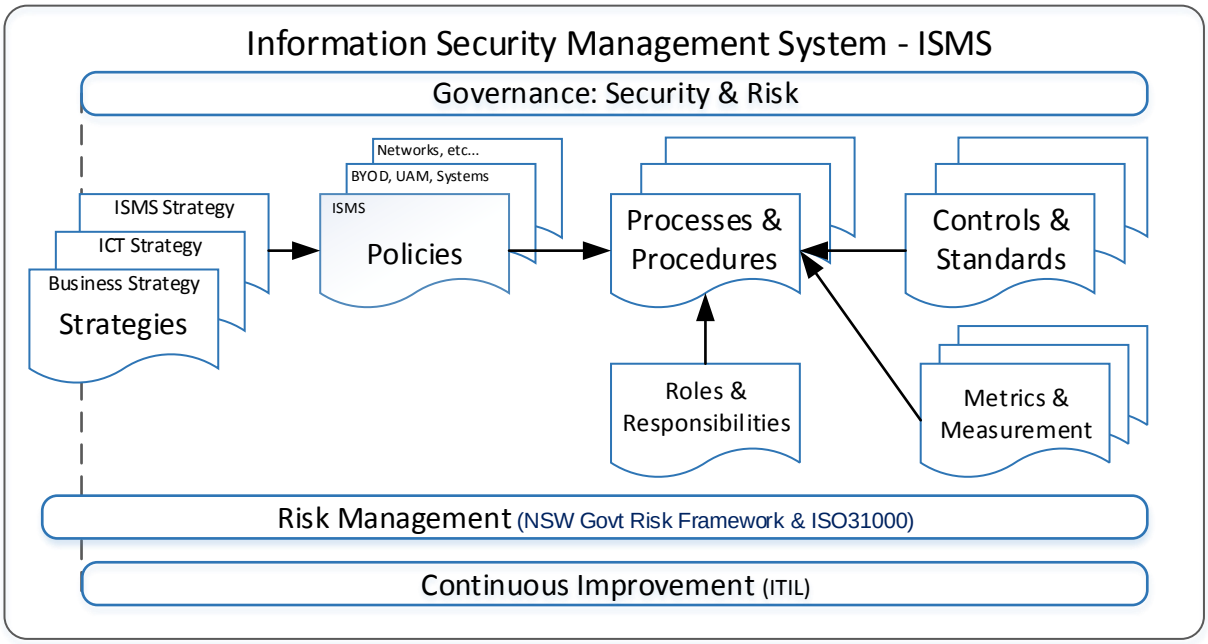

Figure 2. Information Security Management System architecture – IS

The scope of the ISMS facilitates secure digital assets (information services and infrastructure) that is owned, operated or managed by ISLHD.

The ICT services within scope, whether the services are subcontracted to service providers or managed internally by departments are:

a) Customer Services;
b) IT Services;
c) Application Support Services;
d) Technical Services;
e) Clinical Technology Centres;
f) Corporate Technology Centre;
g) Government Data Centre Services;
h) Infrastructure and Security architecture.

2.2 ISMS Review

The ISMS and other related technical policies must be reviewed annually by the ISGC as part of the DISP and ISO27001 to;

a) Ensure Consistency with Laws, Regulations, NSW Cabinet mandates and NSW Government Digital Information Security Policy (DISP);
b) Assess the impact to business by the policies and resulting risk;
c) Align the ISMS to the strategic business and security objectives of ISLHD;
d) Ensure the Information Security policy is clear, concise, and SMART (Specific, Measurable, Attainable, Relevant and time-related).

The outcomes of the review will be reported in the ISGC meeting minutes and the review is acknowledged in the annual attestation as per the NSW Government DISP reporting criteria.

2.3 ISMS Exemptions

Any exemptions to the Information Security Policy or associated technical policies must be approved by the Chief Information Officer (CIO) or designated Senior Information Security Officer (SISO) after a risk assessment has been completed, reviewed and approved by the Information security Governance Committee (ISGC).

Written approval for exemption must be completed through a Brief and must be recorded within the Document Management System (i.e. Content Manager) as per the ISLHD Records Management Standard.

3. TARGET AUDIENCE

This Policy applies to all parties including permanent, temporary casual staff of Illawarra-Shoalhaven LHD, staff seconded from other organisations, contingent workers including labour hire, service providers and professional services contractors and consultants who may utilise ISLHD infrastructure and/or access ISLHD information systems and applications (including systems provided by external providers such as eHealth) with respect to the security and privacy of information.

4. ISLHD RESPONSIBILITIES

In any organisation, dual responsibilities are held by individuals to increase efficiency and reduce costs. The main reason for calling out separate titles and duties is so that the accountability and responsibility for the set of duties associated with a role can be transferred when the prime holder of the role is on leave or a re-organisation occurs as the organisation grows and a transfer needs to occur.

4.1 Executive Policy Sponsor

The Executive Policy sponsor is the owner of the security policy (this document) and is accountable for:

a) Reviewing and recommending changes and alignment to the strategy and business requirements when implementing the Information Security Policy;

b) Analysing the proposed changes to the ISMS policies and the resulting business impact;

c) Approving proposed changes to the ISMS policies;

d) Overseeing the review and approval of Information Security Policy and process exceptions and;

e) Presentation of the security posture, risks and threat landscape to the ISLHD Information Security Governance Committee (ISGC).

4.2 ICT Specialist Systems Managers

All Managers are individually responsible for ensuring that the policy is communicated to and understood by staff.

4.3 ISLHD Staff and Contractors

All staff are responsible for information security and therefore must understand and comply with this policy, the supporting ISMS technical policies and NSW Health Code of Conduct. Failure to do so may result in disciplinary action.

Contracts with external contractors that allow access to the organisation's information or systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

5. COMPLIANCE AND REPORTING

5.1 ISMS Compliance Objective

Compliance and reporting is mandated in the NSW Government DISP which require an annual audit to be completed by 30th June each year and an attestation to be published in the ISLHD's annual report.

The object of the reporting is to:

a) Determine the current state of the IS in relation to the DISP;

b) Document any areas that requires remediation and develop an action plan to address the issues;

c) To show that an Information Security Management System is in place, is active and;

d) Reporting and evidence gathering supplies proof of compliance.

5.2 ISMS Compliance Scope

Business owners or managers who have digital assets under their management or supply ICT services will give input and report on their compliance as part of the annual attestation.

It is the responsibility the business owners or managers of digital assets to ensure that their digital assets, associated processes, and staff meet compliance requirements.

As part of the compliance verification, evidence generated during the execution of policies and processes must be stored for auditing purposes. Evidence can be any one of the following artefacts and must satisfy the characteristics listed below:

a) Emails;

b) Logs;

c) Output from processes;

d) Trouble tickets;

e) Test outputs from processes;

f) Meeting Minutes from review committees;

g) Authority sign offs and;

h) And other artefact that confirms that an action has been taken and has delivered the desired outcome.

5.3 ISMS Compliance Characteristics

The procedure of compliance evidence must possess the following characteristics:

a) **Verifiable:** it must be possible to confirm the veracity of the conclusions drawn out from the analysis or process carried out.

b) **Reproducible:** all the tests carried out throughout the process must be reproducible at all times.

c) **Documented:** the whole process must be correctly documented and must be carried out in a comprehensible and detailed way.

d) **Independent:** the conclusions obtained must be the same, regardless of the person who carries out the process and the method used.

5.4 ISMS Compliance Characteristics of Evidence:

a) **Admissible:** it must have value.

b) **Authentic:** it must be true and not manipulated in any way.

c) **Complete:** it must represent the evidence from an objective and technical point of view, without personal valuations or prejudices.

d) **Credible:** it must be understandable.

e) **Reliable:** the techniques used to obtain evidence must not generate any doubts as to its veracity and authenticity.

They can be classified in two types:

a) **Physical evidence:** refers to computing material such as: hard disks, pen drives, etc.

b) **Digital evidence:** corresponds to information stored in electronic evidence.

Each process must have specified the following;

a) Entry Criteria.

b) Inputs.

c) Outputs.

d) Exit Criteria.

e) Key performance Indicators.

f) Record Control.

g) ISO 27001 References.

h) Document References.

5.5 ISMS Compliance Responsibility

The responsibility for the generation of compliance to the DISP, shall rest with the business manager of each digital service.

6. INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

6.1 Training & Awareness Objective

The purpose of Information Security training is to educate staff in the daily application of Information Security principles and practices and how the practices can assist in safeguarding the ISLHD digital assets.

People must be able to demonstrate the appropriate skills and competencies required to support Information Security where their work interacts with digital assets to warrant that all activities are completed successfully and correct Information Security decisions are made.

Awareness of the ISLHD Security Policy must be brought to the notice of and made available to all authorised users.

6.2 Training & Awareness Scope

All employees within ISLHD and, where relevant, contractors must receive appropriate awareness education, training and regular updates in organisational policies and procedures, as relevant for their job function.

Staff must be provided access to information security training at the commencement of their employment with refresher updates annually. Training can be delivered by any communications avenue that will support the staff in gaining awareness.

In addition to information security training on the correct application of Information Security to digital assets, users must be equipped by way of training to support the ISLHD's Information Security Policy in the course of their normal work. Users of ISLHD digital assets must not subvert ISLHD information security measures.

6.3 Training & Awareness Implementation Guidance

An information security awareness programme must be established and are aligned with ISLHD's information security policies and relevant procedures while taking into consideration the ISLHD's information to be protected.

The awareness programme must be planned appropriate to the employees' roles within ISLHD, including contractors and volunteers where using digital assets. The activities in the awareness programme should be scheduled at least annually so that the activities are repeated and cover new employees and contractors.

The awareness programme should also be updated regularly so it stays aligned to ISLHD policies and procedures, and should be built on lessons learnt from information security incidents.

Information security education and training should also cover general aspects such as:

a) Stating management's commitment to information security;

b) The need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;

c) Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organisation and external parties;

d) Basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks);

e) Contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

7. INFORMATION SECURITY RISK MANAGEMENT

7.1 ISMS Risk Objective

Risk management provides the ability to assess the value and priority of potential threats and identify mitigating actions to reduce a risk to acceptable tolerances.

The application of risk management is a mandatory requirement of the NSW Government as part of the DISP and for ISLHD it is formalised within Risk Management – Enterprise Risk Management Policy and Framework - NSW Health PD2015_043, and Enterprise Risk Management System (ERMS) Procedure ISLHD OPS PROC/42.

ISLHD departments and ICT service providers that manage digital assets must adopt risk management practices to cover all areas of information security activities across the organisation based upon the NSW Health Framework, NSW Government Risk Management guidelines TPP12-03b and supported by AS/NZS ISO31000:2009.

7.2 ISMS Risk Management Scope

ISLHD departments and ICT service providers that host digital assets must utilise the approved NSW Health Risk Management Framework and ISO31000 Risk Management Principles and Guidelines as a reference when selecting and implementing information security controls, and in evaluating and treating information security risks as part of a formal risk management process.

Reviews of ISLHD Information Security Risk Management must be conducted by the ISLHD ISGC at least annually or when circumstances change.

7.3 ISMS Risk Assessment

Risk assessment processes must be utilised when a change is introduced or new systems are being implemented. Mitigation actions and treatments identified must be communicated to the relevant risk owners for acceptance and action. To achieve this, in line with the Framework, risks must be entered into ISLHD's Enterprise Risk Management System (ERMS) with appropriate treatments and action plans identified, reviewed in accordance with system requirements and

closed out as appropriate. The Enterprise Risk Management System Administrator should be contacted where questions of process arise.

As Risk Management within ISLHD has a specific mandate and function, documents Enterprise Risk Management System (ERMS) Procedure ISLHD OPS PROC/42 and Risk Management – Enterprise Risk Management Policy and Framework - NSW Health PD2015_043 should be referenced for comprehensive guidance and to obtain the required tools.

8. INFORMATION SECURITY IN PROJECT MANAGEMENT

8.1 ISMS in Project Management Objective

Information security must be addressed at the commencement of a project regardless of the type of the project.

8.2 ISMS in Project Management Scope

Information security must be integrated into all projects to ensure that information security risks are identified and addressed as part of a project. This applies to all projects regardless of its character, e.g. a project for a core business process, ICT, facility management and other supporting processes. The project management methods at a minimum must ensure that:

a) Information security objectives are included in project objectives;

b) An information security risk assessment is conducted at an early stage of the project to identify necessary controls;

c) That the risk posture is determined;

d) Information security is part of all phases of the applied project methodology;

e) A risk workshop is conducted at stage gates or when appropriate to ensure that the risks are current and to capture any new risks;

f) Any business processes that are identified for change are considered in view of information security;

g) An Information Security Management plan is developed for the delivered product or service;

h) Information Security acceptance testing is conducted and;

i) Information Security certificates are issued prior to go-live.

9. INFORMATION SECURITY DOCUMENTATION

9.1 ISMS Information Security Documentation Objective

Documentation on how Information Security is applied and managed on a service or application must to be available so that managers can apply the correct controls to secure the service or application with the aim of assuring Information Security compliance.

The documentation is to outline the security posture of the application or service in its default configuration and steps required to meet the LHD minimum set of Information Security controls.

Digital assets that are currently in Business as Usual (BAU) mode must have the information security documents developed and registered with the managers of the digital asset and supporting Information Security department.

9.2 ISMS Information Security Documentation Scope

This scope covers all ICT services; products and applications within ISLHD which must be configured to meet the minimum Information Security requirements. Information Security documents must be available for the managing ICT service and the documentation must be available before the services/system goes live.

ISLHD departments and ICT service providers (including vendors) shall determine the boundaries and applicability of the information security to establish if the Information Security scope has been met in alignment with the DISP.

The documents must be available as documented information in ether MS Word or .PDF format.

9.3 ISMS Information Security Document Contents

For all systems, the security documents or contents relating to security must specify but not be limited to;

a) Administration defaults and how to change the defaults including passwords and access portals;

b) Communications protocol ports that are open or closed and authentication information;

c) Past patches list and bugs that were fixed;

d) Current version and patch status;

e) Forums and community groups;

f) Security best practice;

g) Critical processes for monitoring and;

h) Default Security KPIs and metrics.

9.4 Information Security Management Plan

All services must have an Information Security Management Plan (ISMP) accompanying the security information documentation that governs the integrity, privacy, security, and confidentiality of information, especially highly sensitive information, and the responsibilities of departments and individuals for information stored on the service.

10. INFORMATION SECURITY ROLES AND STRUCTURES

10.1 ISMS Roles & Responsibilities Objective

The defining and separation of information security function(s) for a service or application is a key factor in enhancing the organisation's ability to protect information.

10.2 ISMS Roles & Responsibilities Scope

The defining of roles, responsibilities and structure must be in alignment with the NSW Government DISP and ISO/IEC 27001:2013(E) Section 5.3, roles and responsibilities relating to positions that have a security impact and must be separated from daily administration duties.

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the ISLHD's digital assets.

In some cases, the segregation of duties may be difficult to achieve, but the principle should be applied as far as is possible and practicable with mitigating controls put in place such as monitoring of activities, audit trails and management supervision should be considered.

10.3 ISMS Roles & Responsibilities Implementation Guidance

Job roles should be defined so that no single person can access, modify or use assets without authorisation or detection. For example, the initiation of an action should be separated from its authorisation. The possibility of collusion should be considered in designing the controls and access associated with the service.

10.4 ISMS Roles & Responsibilities Standard

ISLHD must ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

ISLHD or the business service owner or provider must assign the responsibility and authority for:

a) Ensuring that the information security management system in relation to services conforms to the requirements of the NSW Government DISP and;

b) Reporting on the performance of the information security management system to the designated executive.

NOTE: The business service owner may also delegate responsibilities and authorities for reporting performance of the information security management system within the organisation.

The delegation of authority must be measured against risk and be accompanied with a Risk Assessment and Plan with sign off from the ISGC on the residue risk.

Individuals with allocated information security responsibilities may, if permitted, delegate security tasks to others. Nevertheless, the Senior Information Security Officer (SISO) or business owner remain accountable and should determine if delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated in the Risk Plan. In particular the following should take place:

a) The assets and information security processes should be identified and defined;

b) The entity responsible for each asset or information security process should be identified and the details of this responsibility should be documented;

c) Authorisation levels should be defined and documented;

d) To be able to fulfil responsibilities in information security, the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments and;

e) Coordination and oversight of information security aspects of supplier relationships should be identified and documented.

10.5 Solution and Security Architect

The Solution and Security Architect is a Health ICT appointee reporting to the Health ICT Deputy Director. 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 Health ICT and will authorise solutions before build work commences.

10.6 Senior Information Security Officer (SISO)

The Senior Information Security Officer (SISO) position exists to:

a) Have overall responsibility for the management of information security efforts;

b) Advise on application and system information security controls, infrastructure information security, access management, threat and incident;

c) Manage, risk management, awareness programs, metrics determination and assist with vendor assessments;

d) Provide advice and assist in the decision making in relation to the ISLHD’s ICT security posture;

e) Provide security advice to ICT projects to ensure designs meet the requirements of the Information Security Management System policies, controls and standards;

f) Develop policy and accreditation of documentation for submission to the ISGC;

g) Ensure the accreditation of ICT systems is maintained and security documentation remains current;

h) Provide high level technical support for the management of the ISLHD’s security cross domain and gateway systems;

i) Provide support in managing the Public Key Infrastructure (PKI) environments.

j) Act as secretariat to the ISGC;

k) Coordinates the development of Information Security Management System (ISMS) and Risk policies for ISLHD;

l) Implement the Information Security Management Strategy;

m) Implement hierarchical information and decision escalation procedures;

n) Monitor regular and routine mechanisms for ensuring that the use of information security measurement systems complies with information security-related legislation and regulation.

o) Analyse overall implications of the changing threat landscape;

p) Develop an Information Security Plan that identifies the information security environment and activities to be implemented by the project team to protect organisational assets;

q) Ensure that the potential impact of changes is assessed and;

r) Collect and analyse performance and compliance data relating to information security and information risk management.

11. ISMS GOVERNANCE

11.1 ISMS Governance Purpose

Governance ensures that stakeholder needs, conditions and options are evaluated to;

- Determine balanced, agreed-on enterprise objectives to be achieved;
- Set direction through prioritisation and decision making and;
- Monitor performance and compliance against agreed-on direction and objectives.

11.2 ISMS Governance Scope

The governance objectives of benefits realisation, risk optimisation and resource optimisation, include practices and activities aimed at evaluating strategic options, providing direction to information security and monitoring the outcome in the Evaluate, Direct and Monitor (EDM) domain in line with the ISO/IEC 38500:2015 Information technology - Governance of IT for the organisation concepts.

The Terms of Reference for the Information Security Governance Committee (ISGC) ensures;

- That a consistent approach that will integrated and aligned with the enterprise governance;
- To ensure that ICT ISMS related decisions are made in line with the enterprise's strategies and objectives;
- ICT ISMS related processes are overseen effectively and transparently;

- Compliance with legal and regulatory requirements is confirmed and;
- The governance requirements for board members are met.

11.3 ISMS Governance Standard

The Information Security Governance Committee (ISGC);

a) Provides oversight on policy development, Risk Management and on the ISLHD's use of the ISMS and is accountable for the development of information security policies and procedures;

b) Develop initiatives to educate and protect users, patients and departments relating to Information Security to foster an information security-positive culture and environment;

c) Advise on Information Security and Risk Management;

d) Implement the Information Security Management Strategy and align with the business and ICT strategies;

e) Review all policies and procedures relating to Information Security and Risk management on a regular basis;

f) Continually identify and engage with ISLHD's stakeholders, document an understanding of the requirements and make a judgement on the current and future design of information security governance of digital assets;

g) Monitor the effectiveness and performance of ISLHD Information Security Governance and assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively;

h) Raise the profile of the information security function within ISLHD and outside the ISLHD where required;

i) Provide input to the overall enterprise business continuity management endeavour and;

j) Provide overall decision-making authority over information security domain practices.

12. CORPORATE & CLINICAL APPLICATIONS

12.1 Corporate & Clinical Applications Objective

The objective is to ensure that corporate or clinical service's or application's Information Security requirements are considered by the business owner or manager of the service or application and that Information Security is assessed, documented and applied as part of the service or application lifecycle.

12.2 Corporate & Clinical Applications Scope

For new system or services delivering a corporate or clinical service, the systems must undergo analysis in terms of Information Security requirements. The request for the analysis should form

part of the proposal or tender prior to acquisition to reduce cost and increase the likelihood of project success.

The outcome of the analysis must state the present Information Security posture and the actions that are needed to be taken to meet an end state that is complaint with the LHD Information Security Policy, the NSW Government DISP and ISO27001 requirements.

The analysis and subsequent actions to bring the system into compliance should reflect the value of the information to ISLHD as per the Data Labelling and Classification policy, and the potential damage which might result from a failure or absence of security.

Corporate and clinical services or applications that are in Business as Usual (BAU) mode, must undergo a risk assessment documenting the Information Security posture which then must be submitted to the ISGC for review and risk acceptance. If the risk tolerance is outside the corporate or department limits, then mitigation actions must be taken to bring the service, application or system within the risk tolerance which may include replacement.

The security requirements and controls should reflect the value of the information involved to ISLHD, and the potential damage which might result from a failure or absence of security. Areas which can be considered include but not limited to:

a) Segregation of facilities or duties;

b) Access controls for information systems files and functions;

c) Validation of input data, Design and use of controls;

d) Creation and regular review of audit trails for critical events and attempted unauthorised access;

e) Procedures, documentation and training to allow the system to be used securely by non-specialist staff;

f) Creation and storage of backup copies of data and system;

g) Recovery from failures, especially for high availability applications;

h) Use of data encryption to protect data from unauthorised access, either during transmission or storage;

i) Use of digital signatures to provide message authentication;

j) Use of formal change controls to ensure testing and authorisation of updates;

k) Use of version controls for IT system software and documentation;

l) Protection of test data, by ensuring any production data is “depersonalised” before use and removed after testing and;

m) Restriction on access to system audit tools, to prevent misuse or compromise.

13. SYSTEMS SURVEILLANCE & MONITORING

13.1 Systems Surveillance & Monitoring Objective

As part of ensuring Information Security, all systems regardless of their function are subject to systems monitoring in line with Information Security controls. It is realised that some systems may not be capable of being sufficiently monitored or will accept systems monitoring software in which case, a risk assessment must be conducted to identify mitigating actions and the actions applied.

Systems monitoring ensures a system remains compliant to the LHD Information Security Policy, NSW Government DISP and ISO2700 information security standard.

13.2 Systems Surveillance & Monitoring Scope

Information Systems assets must be monitored to ensure conformity to security standards of Confidentiality, Integrity and Availability (CIA). In order to have effective monitoring and audit tools, it is essential that logging of potentially damaging events – including exceptions, violations and other security-relevant events be performed, monitored and kept for a recommended period of time to be determined by the digital asset manager. Where possible, event logs should include User Ids, dates and times, and node address or terminal identifier.

Monitoring must be integrated at the planning, design, implementation and monitoring stages of a project to include information security procedures and other controls capable of enabling prevention, and prompt detection of security events, and response to security incidents.

13.3 Systems Surveillance & Monitoring Management Practice

Systems Surveillance and Monitoring utilises tools to indicate a change in status of the system under examination.

a) Using intrusion detection tools, monitor the infrastructure for unauthorised access and ensure any events are integrated with general event monitoring and incident management.

b) The information is to be stored sufficiently so that chronological information in operations logs enabled the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

c) Log security-related events reported by infrastructure security monitoring tools, identifying the level of information to be recorded based on a consideration of risk and retain them for an appropriate period to assist in future investigations.

d) Define and communicate the nature and characteristics of potential security-related incidents so they can be easily recognised and their impacts understood to enable a commensurate response.

e) Regularly review the event logs for potential incidents.

f) Maintain a procedure for evidence collection in line with best practice forensic evidence rules and ensure that all staff are made aware of the requirements.

g) Ensure that security incident tickets are created in a timely manner when monitoring identifies potential security incidents.

14. MALICIOUS SOFTWARE MITIGATION

14.1 Malicious Software Mitigation Objective

Implementing anti-malicious software assists to ensure that information and information processing facilities are protected against malicious software or malware.

14.2 Malicious Software Mitigation Scope

Anti-malicious software must be applied to all systems to prevent the systems from being compromised and provides recovery controls. The following guidance must be considered in maintaining protection and managers of digital assets must:

a) Conduct regular reviews of the software and data content of systems supporting critical business processes to ensure that the systems has not been compromised. The presence of any unapproved files or unauthorised amendments should be formally reported and investigated;

b) Installing and ensuring regular updates of malware detection and repair software that will scan digital assets and media as a precautionary control on a routine basis;

c) Implement scanning on:

1. Any files that are received over networks or via any form of storage medium;
2. Electronic mail attachments and downloads;
3. Web pages.

d) Implement scanning at different places, e.g. at electronic mail servers, desk top computers and at network entry points;

e) Define procedures and responsibilities to deal with malware attacks on digital assets;

f) Prepare appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements;

g) Implement procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

h) Implement procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative and;

i) Isolate environments where catastrophic impacts may result.

It is essential that precautions are taken to prevent and detect the currently known forms of malicious software and computer viruses on digital assets which will require planned and tested processes for distributing updates to resolve identified system vulnerabilities.

Virus detection and prevention measures must be implemented on all digital assets including mobile and smart devices that come in contact with the ISLHD infrastructure. Users must be made aware of cyber threats and their responsibilities through awareness campaigns or training.

15. INFORMATION SECURITY COMPLIANCE WITH LEGAL REQUIREMENTS

All digital assets must comply with all relevant contractual and statutory requirements which must be explicitly defined and documented for each digital asset. The specific controls and responsibilities to meet these requirements must be defined and documented in the digital asset management plan. It is the manager of the digital asset responsibility to ensure compliance.

Proprietary software products are usually supplied under a licence agreement that limits the use of the product to specific computers. Users of the software must be made aware of the limitations imposed by the licence agreement and comply with them at the time of receiving guardianship over the digital asset.

A register of software must be maintained for all digital systems and an audit of software in use must be undertaken at least annually. Audits may be conducted by the business managers of the application, service providers or external/internal auditors.

Users must not copy software from one computer to another without the software owners documented consent.

15.1 Vendor Compliance

Vendors who are certified on the NSW Government Tender Panel must comply with;

- NSW Government Digital Information Security Policy;
- NSW Government Information Security Event Reporting Protocol;
- NSW Government Cloud Policy;
- All other applicable NSW Government policies and;
- ISLHD's Information Security Management System (ISMS) and supporting technical policies.

The compliance is referenced in Schedule 1 of the General Order Form, Procure IT Version 3.2, Item 25. Secrecy and Security.

Vendors engaging in supplying digital services with Illawarra Shoalhaven LHD must comply with the above mentioned policies and the Illawarra Shoalhaven LHD vendor compliance policy.

16. DEFINITIONS

ISMS

Information Security Management System (ISMS) is a set of frameworks that contain policies and procedures for tackling security risks in an organisation. The focus of an ISMS is to ensure

business continuity by minimising all security risks to information assets and limiting security breach impacts to a bare minimum.

DISP

The Digital Information Security Policy (DISP) sets out the digital information security requirements for the NSW public sector as mandated by the NSW government.

ISO27001

ISO/IEC 27001:2013 is an information security standard that provides a framework for an information security management system (ISMS).

BAU

Business as Usual: the daily operational activities to maintain information systems.

CIA Triad

The CIA triad of information security is an information security benchmark model used to evaluate the information security of an organisation. The CIA triad of information security implements security using three key areas related to information systems including Confidentiality, Integrity and Availability.

ISMS

Information Security Management System (ISMS) is a set of frameworks that contain policies and procedures for tackling security risks in an organisation. The focus of an ISMS is to ensure business continuity by minimising all security risks to information assets and limiting security breach impacts to a bare minimum.

DISP

The Digital Information Security Policy (DISP) sets out the digital information security requirements for the NSW public sector as mandated by the NSW government.

ISO27001

ISO/IEC 27001:2013 is an information security standard that provides a framework for an information security management system (ISMS).

System

A system may be either one or a conglomeration of;

- Application
- Operating systems
- Server hardware
- Network components

That is configured to supply particular outcomes when interacted with.

Business Owners or Managers

A Business Owner or Manager are the assigned owners and/or managers of digital assets.

Digital Asset

A digital asset may be one or many PCs, Electronics Medical device which can interact with people or other systems, an application such as eMR and the supporting hardware and software, a network device or any conglomeration of assets that come together to produce a system that has a specific business purpose such as managing medical records.

17. DOCUMENTATION

N/A

18. AUDIT

To meet compliance and assurance requirements as set out in the NSW Government DISP, an annual audit of the Information Security Management System (ISMS) must occur. The scope of the audit is to be determined by the auditor with the scope set out in the audit's Statement of Applicability.

19. REFERENCES

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

a) NSW Government Digital Information Security Policy (DISP),
b) Electronic Information Security Policy – NSW Health PD2013_033
c) NSW Information Classification and Labelling Guidelines
d) SESLHD ISMS Strategy 2017-2022
e) Risk Management – Enterprise Risk Management Policy and Framework – NSW Health PD2015_043
f) Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).
g) Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).
h) NSW Government ICT Strategy 2015
i) Enterprise Risk Management System (ERMS) Procedure ISLHD_OPS_PROC/42
j) GIPA - Government Information (Public Access) Act 2009

19.1 Standards

a) ISO 27001:2013 Information technology - Security techniques - Information security management systems.

b) ISO/IEC 27002:2013. Information Technology - Security Techniques - Code of Practice for Information Security Management.

c) ISO 27014 Information technology – Security techniques – Governance of information security

d) ISO 31000 Risk management - Principles and guidelines

e) ISO/IEC 38500:2015 Information technology - Governance of IT for the organisation

19.2 Supporting Documentation

a) Australian Government Cyber Security Strategy

b) Australian Signals Directorate: Australian Government Information Security Manual

c) Australian Signals Directorate: Strategies to Mitigate Targeted Cyber Intrusions

d) Australian Signals Directorate: Top Four Mitigation Strategies to Protect Your ICT System

e) Australian Government Attorney-General's Department Protective Security Framework

f) Cobit 5 for Information Security

g) ISACA Overview of Digital Forensics

8. REVISION & APPROVAL HISTORY

Date	Revision No.	Author and Approval
May 2018	**0**	Program Manager ICT Security & Strategy.
August 2018	**0**	Executive Director Corporate Services, Assets and Chief Information Officer