SESLHD POLICY COVER SHEET

NAME OF DOCUMENT	Internet of Things (IoT) Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/312
DATE OF PUBLICATION	June 2019
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Standard 1 – Governance for Safety and Quality in Health Service Organisations ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems
REVIEW DATE	June 2024
FORMER REFERENCE(S)	None
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Flora Karanfilovski Director, Health ICT / CIO, SESLHD
AUTHOR	Shane Feeney
POSITION RESPONSIBLE FOR THE DOCUMENT.	Program Manager, ICT Security & Strategy Health ICT Shane.Feeney@health.nsw.gov.au
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, Patch Management.
SUMMARY	This document provides the overarching policy under which information devices called IoT systems should have security controls applied in the South Eastern Sydney Local Health District

Internet of Things (IoT) Policy SESLHDPD/312

1. Policy Statement

The purpose of the Internet of Things (IoT) Policy is to describe the principles used to manage and protect assets that SESLHD departments manage, from deliberate or inadvertent unauthorised acquisition, damage, disclosure, manipulation, modification, loss or use.

The policy focuses on establishing a trusted environment for IoT and leverage off the SESLHD Information Security (InfoSec) controls by providing a trusted, safe, secure, compliant and best practice environment for IoTs.

2. Aim

This Internet of Things (IoT) Policy provides management direction and supports applying Information Security (InfoSec) across the District on devices that are classified as IoT devices.

3. Target Audience

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

4. Internet of Things Policy Scope

The IoT Policy applies to all devices that meet the definition of an IoT device as outlined in Section 5 - Definitions.

The following principles are to be applied to IoT devices and are the minimum requirements required for an IoT device.

This policy does not cover devices that are not attached to the SESLHD network infrastructure.

4.1 Attachment of IoT Devices to the SESLHD Infrastructure

Prior to attaching an IoT device to the SESLHD infrastructure, a risk assessment and device classification must be conducted and approval for attachment to the SESLHD network infrastructure by the Information Security Governance Committee (ISGC), or delegate must be sought.

To engage Health ICT to assist with the risk assessments, a request can be logged with the eHealth State Wide Service Desk (SWSD).

4.2 Class Classification and Assessment

All IoT devices must be classified as listed below, as this will allow for the appropriate plans to be developed by the managers of the device in the event that a failure occurs. By classifying the device, an impact to the department and the district can be quantified and the appropriate response taken.

The classification is a risk assessment and as such, aligns with the NSW Ministry of Health Risk Management Framework which can be referred to for guidance.

The classes for the IoT devices are;

Class 0: Where compromise to the data generated, or loss of control, is likely to result in little discernible impact on an individual or organisation.

Class 1: Where compromise to the data generated, or loss of control, is likely to result in no more than limited impact on an individual or organisation and the impact can be actively managed.

Class 2: In addition to class 1, the device is designed to resist attacks on availability that would have significant impact on an individual or organisation, or impact many individuals, for example by limiting operations of an infrastructure to which it is connected.

Class 3: In addition to class 2, the device is designed to protect sensitive data, including sensitive personal data.

Class 4: In addition to class 3, where compromise to the data generated, or loss of control, has the potential to affect critical infrastructure or cause personal injury.

Class 5: In addition to class 4, where compromise to the data generated, or loss of control, will affect critical infrastructure or cause multiple injury.

Table 1. Compliance Class Security Objectives

Compliance Class	Security Objective		
	Integrity	**Availability**	**Confidentiality**
Class 0	Minimal (or Basic)	Minimal	Minimal
Class 1	Minor (or Medium)	Minor	Minimal
Class 2	Minor	Major	Minor
Class 3	Moderate	Major	Major
Class 4	Major (or High)	Major	Major
Class 5	Catastrophic	Catastrophic	Catastrophic

Definitions of the levels of integrity, availability and confidentiality are as follows:

Integrity

- Minimal – devices or services that malfunction, that would cause a minimal or negligible impact on an individual or organisation.
- Minor - devices or services that malfunction, would have a minor impact on an individual or organisation, requiring attention within the next business day.
- Moderate – devices or services that malfunction would have limited impact on an individual or organisation.
- Major – devices or services that malfunction would have a significant impact on an individual or organisation.
- Catastrophic – devices or services that malfunction would have a critical impact on individuals or organisation.

Availability

- Minimal – devices or services whose lack of availability that would cause minimal disruption.
- Minor - devices or services whose malfunction would have a minor impact on an individual or organisation, requiring attention within the next business day.

- Moderate – devices or services whose lack of availability would have limited impact on an individual or organisation.
- Major – devices or services whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals.
- Catastrophic – devices or services whose lack of availability would have a critical impact on individuals or organisation.

Confidentiality

- Minimal – devices or services processing public information.
- Minor - devices or services that malfunction would have a minor impact on an individual or organisation, requiring attention within the next business day.
- Moderate – devices or services processing sensitive information, including personally identifiable information, whose compromise would have limited impact on an individual or organisation.
- Major – devices or services processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation.
- Catastrophic – devices or services processing very sensitive information, including sensitive personal data whose compromise would have a critical impact on individuals or organisation.

4.3 Service Provision and Privacy

As part of the service, the IoT device service providers must demonstrate that they will be complying with the privacy principles for corporate and patient data in line with the NSW Government privacy legislation and the SESLHD Policy Directive SESLHDP/315 - Data Labelling and Classification Policy.

The following principles must be affirmed by the vendor/ service provider and confirmed by the department manager of the devices before installation.

Service Provision and Privacy

- Appropriate technical and organisational measures are taken by the vendor/ service provider to safeguard security of the service and data handling, if data is sent to them;
- A mechanism for risk notification from the vendor/ service provider to the department manager of pending threats, or newly identified vulnerabilities;
- Appropriate process is in place for managing data breaches and notification of a breach by the vendor/ service provider to the manager;
- The highest privacy settings must be the default configuration for an IoT device; and
- The service provider must indicate the purpose of the use of data that has been received.

Data

Where data is sent to the service provider for storage, or data is stored off site;

- Data segmentation and classification occurs at the service provider data storage in line with SESLHD Policy Directive SESLHDPD/310 - Information Security Policy.

- If the data is stored in virtualised environments, classification is to occur in line with SESLHD information security policies, and the virtualised environment is secure.
- Consent must be obtained if the service provider is to use the data other than what it is intended for.
- Data minimisation occurs is only to request, collect, obtain, derive and process data to the extent necessary (need-to- know principle) by the service provider.
- Opt-out of data transmission option must be available to the SESLHD department manager.
- Data ownership is perpetually retained with the SESLHD department.
- Subscriber (department) data is isolated from other subscribers at the service provider data storage premises.
- That data context is employed to affirm data source incontestability and authenticity.

Encryption

Where the data is sent externally for processing and is non-public data, the following controls must be exercised;

- Encryption should be the default position and applied at all stages of handling data, including in communication (local and internet), storage of data at rest, storage of keys, identification, access, as well as a secure boot process.
- Data should be encrypted on the application layer using end-to-end security, cryptographic principles, and key management should be documented with the documents submitted to SESLHD Health ICT for acceptance when the device under goes an information security review.

Compliance and Risk

Where the IoT sends data to a service provider for interpretation and storage, the service provider is responsible for compliance.

- **Compliance and accountability:** Service providers are accountable for meeting the Australian federal and NSW state government's legislative and mandated requirements, contractual and ethical compliance, as well as for any misuse of collected personal data. If the data is compromised, lost, unlawfully disclosed or accessed, the vendors must formally notify their client; the SESLHD Department who hosts the IoT within the district, of the compromise and the impact as soon as possible.
- **Risk impact assessment by design:** The service provider must carry out an assessment of the risk of data being compromised, disclosed, accessed or lost. Likewise, an assessment of the consequences from regulatory, contractual and ethical perspective should be carried out.

Risk assessments must be conducted using the NSW Treasury Risk Management Methodology.

Secure Design and Updates

To ensure that devices continue to meet information security controls and protect against new threats, the devices must adhere to the following controls;

- **Security by default:** The vendor/ service provider must ensure that the most secure, proven, well understood and securely updateable settings, are applied before starting operations and during IoT life time.
- **Secure updates:** That trusted and transparent updates should only be provided by authorised parties.
- **High-level secure baseline:** A high level secure baseline should be applied when safety is at stake or safety can be materially impacted.
- **Safe and secure interactions:** The vendor/ service provider must implement and validate safety principles, separately from security principles and provide documentation of the validation to the department.
- **Authentication of identities:** Between the IoT device and the end point application, authentication of identities must occur and use common technologies.

IoT Device Assurance

To ensure the IoT device is securely maintained, the vendor/ service provider, along with the manager of the device are to ensure that;

- **Assurance:** The IoT device must have a device maintenance plan for the entire life cycle and the vendor/ service provider must provide end of life guarantees for vulnerabilities notifications, updates, patches and support.
- **Defined functions:** The vendor/ service provider must ensure that IoT devices are only able to perform documented functions, particular for the device/service.
- **Secure interface points:** The vendor/ service provider must identify and secure any non-secure interface points to reduce the risk of security breach.
- **Authentication of identities among themselves:** IoT device communications and authentication use common technologies and applications.

4.4 Compliance Reporting and Monitoring

IoT devices must, where possible, be monitored to ensure that the patches and firmware upgrades have been applied. SESLHD ICT may use an automated mechanism for reporting the patching compliance of systems that are in the SESLHD domain.

IoT devices that cannot be actively monitored must have a schedule determined by the risk assessment that would determine the frequency of the checks.

ICT specialists that manage IoT devices, not under SESLHD ICT management, are responsible for confirming the patch compliance of their systems and taking prompt remedial action where IoT devices are found to not be fully up to date.

Security patching status must be reported to the SESLHD Information Security Governance Council at least annually. This can be done by emailing the status to the SESLHD CIO and district departments can seek assistance on the report format and types from Health ICT by lodging a request via the eHealth State Wide Service Desk.

5. IoT Device Information Security Documentation

5.1 IoT Security Documentation Purpose

A record/library must be maintained in relation to IoT device information security so that it provides;

- Assurance that the device is, or can be secured;
- How to secure the device; and
- Service providers must document the security settings and how to administer the IoT device and give a copy to the SESLHD department installing the device(s).

5.2 IoT Security Document Contents

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

- Administration defaults and how to change the defaults including passwords and access portals;
- Communications protocol ports that are open or closed and authentication information;
- Past patches list and bugs that were fixed;
- Current version and patch status;
- Forums and community groups that the department can join so as to gain a better understanding of the device and its operation;
- Security best practice for the device and the preferred default configuration;
- Critical processes that should be monitored; and
- Default Security KPIs and metrics.

5.3 Security Management Plan (SMP)

All IoT devices must have a Security Management Plan (SMP) accompanying the security information documentation that governs the integrity, privacy, security, and confidentiality of information, especially where highly sensitive information is involved outlining the responsibilities of departments and individuals for such information, typically found in a RACI table. A sample SMP can be obtain from Health ICT by lodging a request with the eHealth SWSD.

5.4 IoT Security Exemptions

Any exemptions to the Internet of Things Policy must be approved by the Chief Information Officer (CIO) or ICT Director after undergoing a risk assessment. 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 SESLHD Records Management Standard.

6. Definitions

IoT – Internet of Things

IoT is a seamless connected network of embedded objects/devices, with identifiers, in which Machine-to-Machine (M2M) communication without any human intervention possible, using standard and interoperable communication protocols.

IoT devices can be any device that can be an interconnected item in an industrial, home or business setting and has the capability to gather current state/information and act on it, or send it to other systems for further analysis. All things or devices, may be attached to sensors that help gather current state/information.

Internet of Things involves three distinct stages:

a) The sensors which collect data (including identification and addressing the sensor/device),

b) An application which collects and analyses this data for further consolidation, and

c) Decision making and the transmission of data to the decision-making server.

RACI

A responsibility assignment matrix, also known as RACI matrix describes the participation by various roles in completing tasks or deliverables for a project or business process. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes.

RACI is an acronym derived from the four key responsibilities most typically used: Responsible, Accountable, Consulted, and Informed.

Security Management Plan (SMP)

A system security plan is a formal plan that defines the plan of action to secure a computer or information system.

It provides a systematic approach and techniques for protecting a computer from being used by unauthorised users, guards against worms and viruses as well as any other incident/event/process that can jeopardise the underlying system's security.

7. Documentation

Procedural documentation for the on-boarding of IoT devices is described in the Internet of Things (IoT) On boarding Procedure.

8. Reference Documents

The following documents are referenced in this policy:

Legislation, Policies and Guidelines.

a) SESLHD Policy Directive SESLHDPD/310 - Information Security Management

b) SESLHD Policy Directive SESLHDP/315 - Data Labelling and Classification Policy

c) NSW Government Cyber Security Policy

d) NSW Ministry of Health Policy Directive PD2013_033 - Electronic Information Security Policy

e) NSW Government Classification Labelling and Handling Guidelines

f) Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

g) Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)

8.1 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 31000 Risk Management - Principles and guidelines

d) IoT Security Compliance Framework. Release 1.1, Dec '17 IoT Security Foundation

9. Revision and Approval History

Date	Revision	Author	Approval
March 2019	DRAFT	Initial draft. Shane Feeney, Program Manager ICT Security and Strategy, Health ICT	Flora Karanfilovski, Director, Health ICT
May 2019	DRAFT	Draft for comment period. No feedback received. Final version approved by Executive Sponsor. Formatted by Executive Services prior to tabling at June 2019 Executive Council meeting for approval to publish.	Flora Karanfilovski, Director, Health ICT
June 2019	1	Endorsed by Executive Council at June 2019 meeting.	