

SESLHD POLICY COVER SHEET



Health
South Eastern Sydney
Local Health District

NAME OF DOCUMENT	Network Security
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/313
DATE OF PUBLICATION	July 2024
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standard: Clinical Governance ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems
REVIEW DATE	July 2029
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR	Director, Digital Health / CIO
AUTHOR	Shane Feeney, Program Manager, ICT Security & Strategy Information Management Services Directorate
POSITION RESPONSIBLE FOR THE DOCUMENT	Awais Vaseer, Head of ICT Risk & Cybersecurity Awais.Vaseer@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, network, infrastructure.
SUMMARY	This document provides the overarching policy under which network security is to be applied to South Eastern Sydney Local Health District infrastructure.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY
This Policy is intellectual property of South Eastern Sydney Local Health District.
Policy content cannot be duplicated.

Feedback about this document can be sent to SESLHD-Policy@health.nsw.gov.au

1. POLICY STATEMENT

South Eastern Sydney Local Health District (SESLHD) recognises that broad clinical access to patient records is necessary, for the safe and effective functioning of an evidence based integrated healthcare system.

SESLHD has statutory and regulatory obligations concerning information security, of which network security is a significant aspect.

The purpose of the Network Security Policy is to describe the principles used to manage and protect SESLHD assets when a network capable device is required to be connected to the network infrastructure.

This policy is a sub-policy to the SESLHD Information Security Policy - SESLHDPD/310. It is recommended this policy is not read in isolation.

2. AIMS

The policy provides information security principles when using SESLHD digital infrastructure and supports applying Information Security (InfoSec) across the SESLHD organisation.

The Network Security Policy principles are:

- Apply the minimum information security controls to data transmission, ensuring security of data in private and public facing networks and the protection of digital services from unauthorised access.
- Ensure information security controls are applied on devices which enable communications across wired and wireless environments such as routers, switches, firewalls, load balancers, Intrusion Detection Devices (IDS), Wireless Access Points (WAPs) and any other devices that provide a network connection.
- By utilising an on-boarding procedure for each network device which must execute to ensure appropriate risk and administration activities are carried out prior to attaching the device or ICT service.

Assistance and guidance can be sought by contacting SESLHD Digital Health by logging a call with the eHealth State Wide Service Desk (SWSD).

3. TARGET AUDIENCE

This policy applies to all parties including permanent, temporary and casual staff of South East Sydney Health, staff seconded from other organisations and contingent workers including labour hire, service providers, professional services contractors and consultants, 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 via the district's network infrastructure.

4. INFORMATION SECURITY POLICY SCOPE

The policy applies to all digital and analogue network infrastructure installed within the District premises, which is used for the transmission of data.

No distinction is made as to the electronic medium on which the information is transmitted, as the policy is intended to be technology independent.

A network device can be one of several types of equipment namely routers, switches, firewalls, access points, lan controller, network admission controller, application controllers, intrusion detection & prevention devices and such. Physical or software defined networking (SDN) based network devices when configured with software, offer a service and are commonly referred to as network service device or service device.

4.1 Network Management

To ensure that the appropriate operational information security controls are applied to the management of the network, managers should separate network operational responsibilities from network security responsibilities.

For example; staff that support day-to-day operations of the network should not be the same staff that perform network security functions. If responsibility separation is not possible, mitigation actions such as recording of network support staff actions when performing a security functions and the reviewing of the recorded log files or other supervisory actions must be executed.

Department managers or users that operate their own network, must adhere to the same information security management, controls and principles that are applied to the District general network.

4.2 Network Access Principles

The following principles apply to the network infrastructure;

- Access to network services is to be restricted to verified users, devices and applications;
- Where an automated process is used to connect remote systems, a suitably secure authentication mechanism which meets the District's information security standards must be used in the process;
- Network connections with external environments must prevent unauthorised access;
- Cross boundary access between internal and external networks is to be secure and must use an information security approved authentication method at the entry points;
- Remote access to SESLHD systems is to be managed as outlined in SESLHDPD/314 - User Access Management;
- Network devices are not to be accessible or managed remotely from the internet. All access to the devices must only be via internal connections.

4.3 Network Service Device Security

- No local user accounts are configured on any network service device and must use approved authentication mechanisms for all user authentication. -SSH without a Virtual Private Network (VPN) application must not be used.
- The administration and service passwords on network service devices must be kept in a secure encrypted form and must be changed from the default when being configured.
- Information security has defined a set of services or features which must be disabled as the default, until secure configuration is implemented as described in [Appendix A – Network Device Services to Disable](#).
- The following services should be disabled unless a business justification is provided and approval from the Information Security Governance Committee (ISGC) is given. Approvals from the ISGC can be sought by logging a call with the eHealth SWSD:

- Cisco or other discovery protocols;
- Dynamic trunking;
- Scripting environments, such as the TCL shell;
- The following services must be configured;
 - Password-encryption;
 - Network Time Protocol (NTP) configured to a LHD standard source;
- All routing updates shall be done using secure routing updates.
- The Simple Network Management Protocol (SNMP) community strings must follow the District approved strings. Default strings, such as public or private must be removed.
- SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- The router must be included in the corporate enterprise management system with a designated point of contact.
- Each network service device, where applicable, must have a warning statement present for all forms of login, whether remote or local such as the example below:
 - *"UNAUTHORISED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*
- Telnet must never be used across any network to manage a router, unless there is a secure communications tunnel protecting the entire communication path.
- Dynamic routing protocols must use authentication in routing updates sent to network neighbours. Password hashing for the authentication string must be enabled when supported.
- The SESLHD ICT router configuration standard defines the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
 - The TCP/IP access list accounting must be enabled to show the type of access to remote connections;
 - Device logging of activities; and
 - Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped.
- Router console and modem access must be restricted by additional security controls. Assistance can be sought from Digital Health by lodging a call to the eHealth SWSD.
- All backups of network devices must be encrypted to ensure privacy and

confidentiality of the backed up information.

- Network service device operating systems need to be genuine, licensed and be up to date. Devices or operating systems must not be tampered with to circumvent security, policy and configuration controls that have been enforced. Any such tampering with the device is strictly forbidden.
- When not being used Wi-Fi and Bluetooth must be turned off to prevent discovery by third parties. All Bluetooth communications should use a unique pass-code. It is not recommended to connect to unsecured Wi-Fi access points, if in doubt, do not connect.
- Network device passwords must be changed at least annually or more frequently as per the risk assessment.
- Restrict access to network devices to an approved list of personnel.
- Ensure that the current software revision levels of network equipment and server environments are in compliance with the security configuration requirements.

4.4 Network Operations Principles

The following principles are to ensure that appropriate controls for the operation of the devices and the network infrastructure.

- Prior to attaching a network service device to the District network infrastructure, the device must comply with SESLHD Digital Health information security controls and standards as per ISO27001:2013 and Australian Signals Directorate (ASD) Essential 8 (where applicable) to ensure the security of SESLHD digital assets.
- The device must undergo an on-boarding procedure of securing and testing. A request can be lodged via the eHealth State Wide Service Desk (SWSD).
- All data traversing the network must have the appropriate information security controls applied as outlined in SESLHD Labelling and Classification of Digital Data Policy - SESLHDPD/315.
- Information passing across SESLHD and public networks must be protected by use of technical measures such as encryption to address the risk of compromise. A risk assessment on the data must be conducted prior to commencement of the service. The risk assessment methodology to be used is outlined in the [NSW Ministry of Health Policy Directive PD2022_023 - Enterprise-wide Risk Management](#).
- Network environments should be segregated corresponding to the risk identified that may be experienced by the asset using the [NSW Ministry of Health Policy Directive PD2022_023 - Enterprise-wide Risk Management](#).
- Network service devices must be registered in the District's Configuration Management Database (CMDB). To register the devices, a call can be lodged with the eHealth SWSD.
- All network infrastructure and service device changes are to be managed via the LHD Change Control procedure. To register a change, a call can be lodged with the eHealth SWSD.
- Information Security Controls must be implemented to protect information network service devices from illegal software. This includes, for example, software designed to circumvent any security controls; i.e. network service devices must not be loaded with unlicensed software or software not intended for the device.
- Network service devices must be monitored and/or be capable of monitoring for signs of

malicious activity. Connections found to be responsible for suspected malicious activity are to be disconnected from the network.

- Network service devices must enforce a local connection policy based on a risk assessment and business requirements.
- Only approved data transmission protocols to be utilised for network connectivity.
- Network service devices must be configured in a secure manner with the default position being of the highest security position.
- Trust mechanisms on the network service devices must be established between devices to support the secure transmission and receipt of information.
- Periodic penetration testing must be carried out to determine adequacy of network protection, based upon the risk assessment and threat level.
- Periodic testing of network service devices security must be carried out to determine adequacy of system protection, based upon the risk assessment and threat level.
- Network service devices must be wiped of any stored data and securely disposed of at the end of their life cycle.

4.5 Bluetooth Devices

Bring Your Own Devices (BYODs) that utilise Bluetooth must be on-boarded prior to accessing SESLHD digital resources, please refer to the SESLHD Policy Directive -ICT Bring Your Own Device Policy SESLHDPD/306 for further information.

Pins and Pairing

When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised.

If your Bluetooth enabled device asks for you to enter your PIN after you have initially paired it, you must refuse the pairing request and report it to the State Wide Service Desk (SWSD) immediately.

Device Security Settings

All Bluetooth devices shall employ ‘security mode 3’ option which encrypts traffic in both directions, between your Bluetooth device and its paired equipment.

- Use a minimum PIN length of 8. A longer PIN provides more security;
- Set the Bluetooth device to hidden or non-discoverable mode;
- Only activate Bluetooth when it is needed; and
- Ensure device firmware is up-to-date.

Unauthorised Use of Bluetooth

- The following is a list of unauthorised uses of SESLHD owned Bluetooth devices:
- Eavesdropping, device Identification spoofing, Denial of Service (DoS) attacks, or any form of attacking other Bluetooth enabled devices.
- Using SESLHD owned Bluetooth equipment on non SESLHD owned Bluetooth enabled devices.

- Unauthorised modification of Bluetooth devices for any purpose.

User Responsibilities

It is the Bluetooth user's responsibility to comply with the principles within this policy and including;

- Bluetooth mode must be turned off when not in use on your device.
- SESLHD data marked Confidential or above must not be transmitted or stored on Bluetooth enabled devices. All exemptions must be seek approval via the Information Security Governance Committee (ISCG) by lodging a request via the eHealth SWSD.
- Bluetooth users must only access SESLHD information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorised for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to SESLHD Digital Health or the SWSD.

4.6 Security Audits

Digital Health (DH) with SESLHD Internal Audit (IA) may perform random audits to ensure compliancy with this and other information security policies. In the process of performing such audits, DH or any other staff must not eavesdrop on any phone conversation.

4.7 Information Security Setting Changes

Security changes are defined as changes to network service device, that may have an impact on the overall security of the network and therefore changes must follow the [Digital Health change management procedure](#). Engagement of change management can be done by lodging a call with the eHealth SWSD.

4.8 Monitoring and Compliance Reporting

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

Prior to attaching a device, a review must be conducted to establish the suitability and capability of the device with regards to monitoring. Assistance can be sought by lodging a call with the eHealth SWSD.

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

IT specialists that manage network devices not under DH management are responsible for confirming the patch compliance of their systems and taking prompt remedial action where Network devices are found to be not fully up to date.

Security patching status must be reported to the SESLHD Information Security Governance Council and Digital Health Director at least annually in line with the NSW Government mandated compliance reporting as specified in the [NSW Cyber Security Policy](#).

4.9 Threat Monitoring and Privacy

Network service device logs must be monitored for malicious activity on a routine schedule, as set by the risk assessment and threat landscape.

Other network traffic may be logged as necessary for troubleshooting and resolution of network issues. Automated scans for unencrypted sensitive data are conducted as set by the risk assessment and threat landscape with findings logged for appropriate management.

Only malicious or extraordinary activity is to be logged, i.e.: management by exception. These measures must not be used for tracking and/or monitoring an individual's network activity.

Confidentiality of all information gathered as a result of network monitoring will be maintained at all times.

Access to information obtained through network monitoring will be limited to authorised staff and in the event of an investigation, SESLHD executive, legal counsel, or law enforcement. The relevant information must be kept in a protected storage area.

Authorised staff must use network monitoring devices only to detect:

- Known patterns of attack or compromise;
- The improper release of confidential employee or patient data;
- To troubleshoot and analyse network-based problems; and
- Ascertain network-based anomalies to determine the security risk to the SESLHD. All monitoring shall be as narrow in scope as possible.

Authorised staff may not exceed specified scope of monitoring (for example, users, address ranges, protocols, and signatures). Only SESLHD Digital Health Networking and the Digital Health Director or delegate may monitor public networks and inter and intra campus networks.

Personnel authorised to analyse network traffic shall not disclose any information realised in the process without approval of the CIO or Digital Health Director.

No authorised personnel shall use network monitoring devices to monitor employee electronic transmissions for job performance evaluation, or as part of an unofficial investigation.

The CIO or DH Director will be the contact for resolution of security-related anomalies or other suspicious activity noticed by representatives of SESLHD DH Networking or in other departments.

All monitoring points will be architected, approved, and configured by SESLHD DH-Networking and the DH Network and Security Architect. Monitoring points and associated devices may not be extended physically or virtually (such as through a VPN) or changed without written approval from the CIO or DH Director. SESLHD DH-Networking shall maintain written records of all monitoring points, architectures, and agreements.

Monitored data and usage logs will not be stored past the period of active investigation. DH-Networking and or the DH Director may store incident related data as required. Unrelated monitored data may not be stored by anyone except as required by law.

SESLHD DH-Networking and or the DH Director may store aggregated data and usage logs for operational, compliance, and statistical purposes. Usage logs must be purged as per SESLHD policies.

Monitoring data stores and log files must not be accessible from the public Internet. DH-Networking personnel must show due care in protection, handling, and storage of all monitored data and logs.

DH Networking and or the DH Director have the authority to discontinue service to any network or network device that:

- Is in violation of this policy;
- Has demonstrated an operational hindrance or threat to SESLHD digital infrastructure; or
- Is a threat to the LHD intranet community in general.

In such cases, DH-Networking or the DH Director shall notify the local IT- Networking Custodian of the disconnection.

In less threatening situations, DH-Networking and DH Director or delegate will contact the local network administrator and inform them of specific actions that must be taken to avoid imminent disconnection. If corrective actions are not implemented as soon as possible, DH-Networking or the DH Director may discontinue service.

All normal requests for monitoring assistance from external agencies or internal departments must be coordinated through the State Wide Service Desk (SWSD).

Digital Health will be responsible for the architecture and operations of all network facilities/ functions required for lawful Intercept assistance and compliance, and will be responsible for executing all requests as coordinated through the DH Director. Departments must comply with all DH requirements and assist Digital Health Networking to fulfil its obligations.

5. WIRELESS DEVICES

5.1 General Requirements

All wireless infrastructure devices that reside at a SESLHD site and connect to a SESLHD network, or provide access to information classified as SESLHD Confidential or higher, must:

- Abide by the standards specified in the Digital Health Wireless Communication Standard;
- Be installed, supported, and maintained by an approved support team;
- Use SESLHD approved authentication protocols and infrastructure;
- Use SESLHD approved encryption protocols;
- Maintain a hardware address (Media Access Control - MAC address) that can be registered and tracked;
- Not interfere with wireless access deployments maintained by other support departments;
- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunnelling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) as the authentication protocol;
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits;

5.2 Wireless Networks Principles

The following directives apply with respect to wireless networks:

- Wireless Access Points (WAPs) connected to the SESLHD network must be approved by Digital Health before installation. To register an installation, a call can be

lodged with the eHealth SWSD.

- All Personnel are strictly prohibited from installing their own WAPs within the SESLHD network;
- Controls over WAPs are to follow the same requirements as for the wired network including, but not restricted to, network registration, malware software, up-to-date patches, and strong passwords that comply with SESLHD Password Policy and Standards;
- Systems using WAPs to access the SESLHD network must have current anti-malware software and up-to-date patches installed;
- Access to SESLHD infrastructure via WAPs must utilise strong authentication and encryption;
- Wireless communications between SESLHD devices and networks must be encrypted;
- Wireless implementations must support a hardware address that can be registered and tracked, i.e. a Media Access Control (MAC) address;
- Effective physical security is to be applied to hardware associated with WAPs;
- WAPs are to be periodically scanned for vulnerabilities to assess the base level of security needed relevant to the network risk.

5.3 Laboratory and Isolated Wireless Device Requirements

All laboratory wireless infrastructure devices that provide access to SESLHD, must adhere to Section 3.1 above. Laboratory and isolated wireless devices that do not provide general network connectivity to the SESLHD network must:

- Be isolated from the LHD network (that is it must not provide any LHD connectivity).
- Not interfere with wireless access deployments maintained by the LHD wireless devices.
- Set the Service Set Identifier (SSID) for the laboratory device different from SESLHD LHD wireless device SSID.

5.4 Home Wireless Device Requirements

There has been recorded incidents of hackers monitoring home networks as an avenue to gain access to the District. As many LHD staff log in from home using their own wireless networks, precautions must be taken to mitigate the risk.

Home wireless infrastructure devices that are used to access to the SESLHD network, must have sufficient security controls enabled to prevent external parties from gaining access and viewing network data. The following are four configuration settings in your home router that must be changed to protect your network:

- Enable Wi-Fi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS;
- When enabling WPA-PSK, configure a complex shared secret key (at least 8 characters) on the wireless client and the wireless access point;
- Change the default SSID name; and

- Change the default Administrator password to a complex password.

If you do not have the skill or knowledge to make the changes, it is advisable to engage your local neighbourhood IT specialist or your telecommunications provider to assist.

6. EXEMPTIONS

Any exemptions to the Network Security Policy must be approved by the Chief Information Officer (CIO) or Digital Health 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.

7. DEFINITIONS

Bluetooth:

Bluetooth is a short-range radio technology (or wireless technology) aimed at simplifying communications among Internet devices and between devices and the Internet.

Configuration Management Database (CMDB):

A Configuration Management Database or CMDB is a database used by an organisation to store information about hardware and software assets (commonly referred to as configuration items [CI]). This database acts as a data warehouse and stores information regarding the relationship between assets, their owners and other critical information used to maintain the device and who to contact in an event of a critical outage.

Denial of Service:

A Denial of Service is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

Dynamic Routing Protocols:

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes.

EAP-FAST, PEAP and EAP-TLS:

Extensible Authentication Protocol (**EAP**) is an authentication framework frequently used in wireless networks and point-to-point connections.

Encryption Mode 3:

All traffic is encrypted using an encryption key based on the master link key. Encryption Modes 2 and 3 use the same encryption mechanism. In addition to the four security modes, Bluetooth allows two levels of trust and three levels of service security.

Firewalls:

A firewall is a system designed to prevent unauthorised access to or from a private network. A firewall can be either hardware or software in form, or a combination of both. Firewalls prevent unauthorised internet users from accessing private networks connected to the internet, especially intranets.

Digital Health:

SESLHD ICT department

InfoSec:

Information Security and or the Digital Health Information Security team.

Intrusion Detection Devices (IDS):

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

Load Balancers:

A load balancer is a piece of hardware (or virtual hardware) that distributes network and/or application traffic across different entry points.

MAC:

Media Access Control Address, a MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and therefore cannot be changed.

Network Time Protocol (NTP):

A networking protocol for clock synchronisation between computer systems over packet- switched, variable-latency data networks.

Password Hashing:

Hashing performs a one-way transformation on a password, turning the password into another string of characters, called the hashed password. “One-way” means that it is practically impossible to go the other way - to turn the hashed password back into the original password.

Patches:

A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug fixes or bug fixes, and improving the usability or performance.

RFC1918:

RFC 1918 was used to create the standards by which networking equipment in a private network assigns IP addresses as there is a limited number of real internet IP addresses. A private network can use a single public IP address to appear as though it is on the internet.

Routers:

A router is a device that analyses the contents of data packets transmitted within a network or to

another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

SESLHD:

South Eastern Sydney Local Health District

Simple Network Management Protocol (SNMP):

Simple Network Management Protocol or SNMP is an Internet Standard protocol for collecting and organising information about managed devices on IP networks and for modifying that information to change device behaviour.

SNMP Community String

The “SNMP Community string” is like a user id or password that allows access to the device's statistics by sending a request and tagging it with the id. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Service Set Identifier (SSID):

A Service Set Identifier or SSID technical term for a network name. When you set up a wireless home network, you give it a name to distinguish it from other networks in your neighbourhood.

Spoofing:

Spoofing is a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage.

Switches or Network Switch:

A network switch (also called switching hub, bridging hub, officially MAC bridge) is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device.

TCL shell:

Stands for Tool Command Language. TCL files are text files containing TCL scripts. TCL is a dynamic open source language used for building web and desktop applications.

TCP/IP:

Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

Telnet:

Telnet is a terminal emulation protocol used on the Internet and TCP/IP-based networks. A Telnet program allows a user at a terminal or PC to log in to a remote computer and run a program and execute other Unix commands.

Wireless Access Point (WAP):

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth.

6. DOCUMENTATION

The following procedures are relative to supporting network security which can be found on the [Digital Health Procedures Portal](#):

- Information Classification Procedure
- Information Transfer Procedure
- Risk Management Procedure
- Unauthorised Access to Network Service Prevention Procedure

7. REFERENCES

The following documents are referenced in this policy:

Legislation, Policies and Guidelines

- [SESLHDPD/310 - Information Security](#)
- [NSW Cyber Security Policy](#)
- [NSW Health Policy Directive PD2020_046 - Electronic Information Security](#)
- [NSW Health Policy Directive PD2022_023 – Enterprise-wide Risk Management](#)
- [NSW Health Policy Directive PD2022_011 - Bring Your Own Device and NSW Health Smart Devices](#)
- [NSW Government Classification, Labelling and Handling Guidelines](#)
- [eHealth Mobile and Smart Device Management Standards \(HS2012_02\)](#)
- [Department of Premier and Cabinet, NSW Government, Policy and guidelines for the use by staff of employer communication devices \(ISBN: 0 7313 3097 8\)](#)

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

8. VERSION AND APPROVAL HISTORY

Date	Version	Version and approval notes
February 2019	DRAFT	Initial draft; Shane Feeney, Program Manager ICT Security & Strategy
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.
June 2019	1	Endorsed at June 2019 Executive Council meeting.
19 July 2024	1.1	Minor review by Awais Vaseer, Head of ICT Risk & Cybersecurity: Updates to reflect change of roles/personnel. reference documents and links and simplification of language. Approved by Executive Sponsor.

Appendix A – Network Device Services to Disable

The following is a list of services that a network device may or may not have, but need to be disabled if they are installed and turned on. Typically home devices have most of these services enabled and need to have the appropriate access controls enabled to make the device more secure.

- i. IP directed broadcasts
- ii. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- iii. TCP small services
- iv. UDP small services
- v. All source routing and switching
- vi. All web services running on router
- vii. Cisco or other discovery protocol on Internet connected interfaces
- viii. Telnet, FTP, and HTTP services
- ix. Auto-configuration