INTERNAL ONLY

ISLHD POLICY COVER SHEET

NAME OF DOCUMENT	Bring Your Own Device (BYOD) Policy
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	ISLHD CORP PD 45
DATE OF PUBLICATION	June 2020
RISK RATING	Low
REVIEW DATE	June 2025
FORMER REFERENCE(S)	N/A
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Chief Information Officer – ICT Services
AUTHOR	User Experience Architect – Health ICT Business Analyst – Health ICT
KEY TERMS	Information security, policy, standard, confidentiality, integrity, availability, privacy, classification, electronic information, compliance, BYOD, Smart Devices, Mobile Devices.
FUNCTIONAL GROUP OR HUB	District-wide
NSQHS STANDARD	Standard one
SUMMARY	This document provides the overarching policy under which BYODs should meet minimum requirements and undergo on-boarding prior to attachment to Illawarra-Shoalhaven Local Health District infrastructure.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

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

Bring Your Own Device (BYOD) Policy

ISLHD CORP PD 45

1. POLICY STATEMENT

ISLHD recognises that access to digital resources when away from a corporate provided device is an important factor in the effectiveness and efficiency of staff which supports greater workplace mobility and flexibility that is enabled by personally owned devices.

A Bring Your Own Device (BYOD) is personally owned device that is enabled to allow access to corporate services and information. This policy only refers to devices that are used and owned by staff.

ISLHD supports and endorses the use of privately and LHD owned devices to access ISLHD's digital resources but prohibits the storage of ISLHD owned information without the device undergoing on-boarding.

2. AIMS

The purpose of the Bring Your Own Device policy is to describe the principles used to manage and protect ISLHD digital resources when a BYOD is attached to the network.

2.1 Scope

The following principles are to be applied to all BYOD devices that are requesting to be attached to the ISLHD's network meet the minimum requirements.

3. TARGET AUDIENCE

All ISLHD staff including Contractors, Contingent Workers, VMOs and Volunteers.

4. PRINCIPLES

All BYOD devices accessing and/or containing information that is owned by ISLHD must be managed and administered through the Mobile Device Management (MDM) system.

ISLHD staff requiring their device to have access to ISLHD digital assets are to raise a request for BYOD Enablement via the SARA Portal to commence on-boarding of the device.

Users are expressly forbidden from storing ISLHD data and/or information on BYOD devices.

4.1 Attachment to the ISLHD Infrastructure

Prior to attaching a BYOD device to the ISLHD infrastructure, the device must comply with ISLHD ICT security controls and standards to ensure the security of ISLHD information assets.

4.2 Smart BYOD Device Security

A hardware level encryption, auto-lock, pin code or equivalent, will be enforced on all BYOD Devices through the MDM system. This provides hardware level encryption and protects the information from privacy or confidentiality compromise if the device is lost or stolen.

Removable storage devices such as Solid-State Drives (SSD), Universal Serial Bus (USBs), Secure Digital (SD) cards or other such storage devices used in conjunction with BYODs must be antivirus scanned and must have encryption enabled.

ISLHD ICT Mobile Device Management (MDM) employs remote wipe technology to remotely disable and delete any data stored on the smart devices which are reported misplaced, lost or stolen.

ISLHD takes no responsibility for any personal or non ISLHD owned information or data that is stored on these devices that may be lost or deleted.

All backups of smart devices must be encrypted to ensure privacy and confidentiality of the backed-up information.

BYOD 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 such as “jail-breaking” or “enabling privileged access” 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 passcode. It is not recommended to connect to unsecured Wi-Fi access points, if in doubt, do not connect.

User must not accept untrusted certificates from websites which will enable insecure browsing.

4.3 Device Physical Security

BYOD devices must not be left unsecured when not attended. Care must be taken when in a public area that the device is secure when not in use, this includes hotel rooms, conference centres and meeting places.

BYOD devices must not be visible in cars and other forms of transport, hotel rooms, conference centres and meeting places when not in use. Where possible, the device should be physically locked away.

At no time is any employee or authorised user working on behalf of ISLHD to provide or share their BYOD credentials or an unlocked BYOD device with access to ISLHD digital assets with anyone.

4.4 Device Loss and Theft

The loss or theft of any BYOD device must be reported immediately to the eHealth NSW Statewide Service desk and the employees line Manager.

The eHealth NSW Statewide Service desk must perform a remote wipe and remove the MDM profile on ISLHD and private devices.

4.5 BYOD Device Software and Updates

BYOD devices operating systems and applications must have the latest updates and approved antivirus application installed prior attaching to the ISLHD infrastructure. Devices are not to be connected if their systems are not up to date.

4.6 Compliance Reporting and Monitoring

BYOD devices must where possible be monitored to ensure that the patches and firmware upgrades have been applied. The MDM will be used for reporting the patching compliance of systems that are in the ISLHD domain.

Security patching status must be reported to the ISLHD Information Security Governance Council (ISGC) and ISLHD ICT Director at least annually.

4.7 Employee Change of Status

When an employee changes their employment status such as; transferring to another department, termination, retirement and/or administrative leave, the manager must immediately notify ISLHD ICT of the change in status so that the employee's profile can be reassigned or terminated. In circumstances where an employee is separating from the District, the Separation Checklist must be completed, evidence of actions are to be recorded in the Districts separation checklist (ISLHD_CORP_F_126_Separation Checklist form) and sent to Workforce Services.

4.8 Device Removal & Disposal

If the owner is intending to change or dispose of their device, it is the responsibility of the owner to immediately notify their manager of the change and owners must ensure secure disposal/ transfer of BYOD.

The manager must immediately notify eHealth NSW State-wide Service where all corporate information must be the wiped from the device using the MDM.

The wiping of the device may inadvertently include non-corporate data of which ISLHD or eHealth carries no responsibility.

Private data backups must also be deleted, and owners must attest to the deletion of the backups. The device must be disposed of securely and safety in compliance with the State Records Authority disposal and retention requirements and in line with NSW Health's Electronic Information Security Policy – PD2013_033.

Scope of Deletion

The scope of deletion applies equally to ISLHD and Owner supplied devices. The remote wipe feature of the MDM Solution will erase all identifiable corporate data from the device including email, calendar, contacts, photos, music, and user's personal files.

Faulty Devices

In cases where the device is faulty and data cannot be removed via its feature set or remotely wiped by the MDM Solution, It is necessary to have the device reset to factory default by ISLHD ICT.

4.9 Device Exemptions

Bring Your Own Device exemptions to the Policy must be approved by the Chief Information Officer (CIO) or Senior Information Security Officer (SISO) after undergoing a risk assessment which is to be reviewed by the ISLHD Information Security Governance Committee.

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

5. DEFINITIONS

Bring Your Own Device (BYOD)

Any end-user computing or smart device that is privately or ISLHD owned, leased or operated by an employee or contractor of ISLHD. It may be an Apple iPad or phone, Android tablet or phone, MS Windows Personal Computer (PC), tablet or phone.

Note: BYOD is a generic term and is often used interchangeably with mobile, smart or end-user computing devices.

Device steward

An individual who has the accountability for care of, or ownership, of an end-user computing device and the applications and data stored on that device.

End-user computing device

Any electronic device which is capable of storing data and connecting to a digital data network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers, thin-clients, wearable technologies, smart watches, woven computing technologies, and netbooks.

Jailbreaking

The process of removing the limitations imposed by Apple on devices running the iOS operating system by hardware/software exploits. Jailbreaking allows iOS (Apple Software) users to gain root access to the operating system, allowing them to download additional applications, extensions, and themes that are unavailable through the official Apple App Store.

Enable Privilege Access

Allowing users of smartphones, tablets, and other devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem

Tethering

Connecting one device to another. In the context of mobile, smartphones and tablet devices, tethering allows sharing the internet connection with a phone or tablet devices with other devices such as laptops. Connection with the phone or tablet with other devices can be done over Wireless LAN (Wi-Fi), over Bluetooth, or by physical connection using a cable for example, through USB

6. DOCUMENTATION

a) ISLHD_CORP_F_126_Separation Checklist form

7. AUDIT

Auditing of the service is conducted by eHealth where ISLHD tenancy is held - through the mobile device security platform as mentioned in the eHealth's Mobile and Smart Device Policy item 5.5.

Where there is a requirement at the local level for reporting it may be requested via the Statewide Service Desk.

8. REFERENCES

Legislation, Policies and Guidelines.

a) ISMS Policy ISLHD CORP PD 38
b) NSW Government Digital Information Security Policy.
c) Electronic Information Security Policy PD2013_033 – NSW Health
d) NSW Government Classification Labelling and Handling Guidelines.
e) Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).
f) Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).
g) eHealth Mobile and Smart Device Management Standards (HS2012_02)
h) eHealth Mobile and Smart Devices Policy (HS/2012_11)

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

9. REVISION & APPROVAL HISTORY

Date	Revision No.	Author & Approval
May 2018	0.0	Program Manager ICT Security & Strategy.
June 2020	1.0	User Experience Architect/ Business Analyst – Health ICT **Approval/Date:** Corporate Policy Recommendation committee/ May 2020 **Approval/Date:** Chief Information Officer / June 2020