HEALTH SERVICES UNION
Bring Your Own Device (BYOD) Policy

Purpose

The Bring Your Own Device (BYOD) Policy provides guidance for HSU staff who would like to use a personally-owned device, such as a smart phone, tablet or laptop, for work purposes. Third party contractors, consultants and partners wishing to use their own devices to connect to HSU network and IT systems are also covered by this policy.

The BYOD Policy forms part of the HSU Policies and Procedures Manual and interacts with the Information Security Policy to protect the users and devices connecting to, or interacting with, HSU's systems and services, and thereby protecting its assets, information and data. Devices covered by this policy include tablets, laptops, smart phones or any device that does not belong to the HSU.

This policy applies to the Union's Leadership team, elected Councillors, employees full-time, part-time, contract, casual and Union delegates of HSU NSW/ACT/QLD. (Collectively referred to as HSU Officials)

Policy

Staff: using your own laptop or tablet for work

There are significant risks associated with using devices for work-related purposes that have the potential to expose sensitive data. Risks are primarily due to the likelihood of devices storing unprotected sensitive data being lost or stolen, use of company unapproved applications and cloud services to handle sensitive data, inadequate separation between work-related use and personal use of a device, and the organisation having reduced assurance in the integrity and security posture of devices that are not corporately managed.

HSU recognises the benefits of mobility and will provide staff with mobile devices that are corporately-managed to enforce policy and technical risk management controls, such as preventing unapproved applications from running and accessing sensitive data; and applying security patches to applications or operating systems in a timely manner. Staff and contractors who have been issued with a corporately-managed laptop or tablet should use it for work, both in the office and remotely. Use of personal laptops and tablets is not supported without prior approval.

Contractors / Third Parties: using third-party devices

Contractors and other partners may use their own devices to access HSU guest WiFi network (internet access only). Use of third-party company-owned devices to access other internally-facing HSU systems, such as the Office 365 Admin portal or firewalls, or to store HSU data will be considered on a needs basis and must be approved in advance by HSU's IT.

BYOD Smartphones

There are several security implications associated with using a personal phone for work purposes. For example, a phone storing unprotected corporate information could be lost or stolen, or personal

phones may not be kept up-to-date with the latest security patches and may be vulnerable to viruses or other malware, providing a 'back door' for malicious agents to access corporate data and systems.

HSU uses cloud-based mobile device management to ensure safe access to corporate data, as follows:

- **Conditional access:** Exchange Online email can be accessed only by compliant iOS and Android devices using the Microsoft Outlook app, enabled with multi-factor authentication.
- **Application protection:** application protection policies may be enforced from the Cloud to, for example, prevent HSU data from being saved to local storage and/or ensure a minimum level of security patching.
- **Device enrolment:** Devices must be enrolled in the HSU's Intune portal; this allows application protection policies to be applied.
- **Selective wipe:** HSU will have the ability to remotely wipe Microsoft 365 email data from Outlook, while leaving any personal email accounts intact.

Staff who have been issued with a HSU phone should use it for mobile access to HSU systems. Staff who do not have a HSU phone may, if they wish, use their own phone to access HSU email but must keep their device up to date with security patches and must accept that HSU will remotely wipe data in the event that the phone is lost or stolen. HSU staff who wish to access their email on personally-owned iOS or Android phones may do so via Outlook for iOS and Android apps.

Staff must seek approval in advance to use a BYOD and phone number reimbursed by the HSU.

Remote Access

Remote access (VPN or using the HSU remote management applications) on a personal device is not recommended. Staff should use their HSU device when accessing systems remotely.

Multi-factor authentication

Multi-factor authentication will be applied whenever HSU systems are accessed remotely, from a third party or personal device.

Any employee identified using a HSU supplied mobile phone in a manner that is unacceptable or inappropriate could be subject to disciplinary action and possible criminal prosecution. Refer to the HSU Mobile Phone Device Policy.

Breaches

Disciplinary action will be taken against a person who breaches the HSU BYOD Policy. Discipline may involve a warning, counselling or dismissal, depending on the circumstances.

Policy Version Control

Policy Approval Date:	2 December 2021
Approved by:	Union Council under Rule 40

Approval Resolution No:	UC 58/2021
Version No:	V1
Replaced Version No & Date:	NA