# Cyber Security Standard – End User Computing

| Version | Approved by | Approval date | Effective date | Next full review |
|---|---|---|---|---|
| X.X | Vice Chancellor | XX Month Year | XX Month Year | Month Year |

| **Standard Statement** | | |
|---|---|---|
| **Purpose** | The purpose of this Standard is to define the minimum cyber security controls to be applied to:<br>a) UNSW-owned end-user devices.<br>b) other end-user devices. | |
| **Scope** | This Standard applies to:<br>a) any person or device (Information Asset) that stores, processes, or transmits UNSW digital information.<br>b) all UNSW digital information.<br>c) any devices (Information Assets) connecting to a UNSW Information Resource. | |
| **Are Local Documents on this subject permitted?** | ☐ Yes, however Local Documents must be consistent with this University-wide Document | ☒ No |
| **Standard** | | |



## 1. Minimum Controls for UNSW Owned Devices

1.1. UNSW owned devices must have the below controls (in Sections 1.2 and 1.3), which may be beyond the minimum required by the *Cyber Security Standard – Risk Management.*

1.2. Devices that are UNSW owned, **must:**

(a) be configured using a baseline configuration (SOE) provided by UNSWIT or a baseline configuration that is compliant with the *Cyber Security Standard – Secure by Design*.

(a) be configured to update with any required security patches, in accordance with the *Cyber Security Standard – Threat and Vulnerability Management.*

(b) be encrypted in accordance with the *Cyber Security Standard – Data Security*.

(c) be configured to require a password, passphrase to log in to the device in accordance with the *Cyber Security Standard - Access Control* or use a strong passcode enabled to protect against unauthorised access.

(d) have UNSWIT Endpoint Detection and Response (EDR) software and other anti-virus software and services installed, in accordance with the *Cyber Security Standard – Threat and Vulnerability Management*.

(e) not be intentionally modified, including where applicable “jailbreaking” or “rooting” a device, or have security software disabled or circumvented.

(f) not have installed unlicensed software.

(g) be recorded in a centralised asset inventory in accordance with the *Cyber Security Standard - Information Asset Management.*

1.3. In addition to the controls in Section 1.2, devices that are both UNSW owned as well as UNSWIT managed, **must:**

(a) be configured using a UNSWIT Baseline Configuration (SOE) or a UNSWIT approved baseline configuration provided by a Cloud Service Provider (CSP) or research partner.

(b) be authenticated via UNSWIT Azure Active directory and have domain-based group policy applied.

(c) ensure access to privileged administrative (sys admin) and elevated business functions is restricted to those with a documented and approved business or technical need. Where there is a business requirement for local administrator access, approval must be provided by Business Owner or delegate and centrally managed by the UNSWIT in accordance with *Cyber Security Standard – Access Control.*

(d) be recorded in the centralised UNSWIT asset inventory.

1.4. Any actual or suspected cyber security event or incident related to a UNSW-owned device must be reported to the UNSWIT Service Desk on (02) 9385 1333 or email itservicecentre@unsw.edu.au**.**

1.5. Information Assets affected by a cyber security event or incident, must not be used during or after a cyber security event or incident. Instructions from UNSWIT must be followed, including, if necessary, the formatting of hard disks.

1.6. Users must at all times employ reasonable physical security measures with Information Assets including UNSW-owned devices. (e.g. not leaving your device unattended in a public environment, not accessing UNSW digital information in public environments where you may be vulnerable to shoulder surfing, not connecting a third-party charger or peripheral device, and not placing the Information Asset in checked luggage).

## 2. Minimum controls for Personal Devices - devices not owned by UNSW (BYOD)

2.1. Personal device used to access, store, process or transmit UNSW digital information, must:

(a) only store UNSW digital information in accordance with the *Cyber Security Standard – Data Security*.

(b) implement all controls required by the *Cyber Security Standard – Risk Management*.

2.2. Users must not perform system administration tasks on any medium or high cyber security risk rated UNSW Information Resource (system or infrastructure), using a personal device.

2.3. For Notebook, Laptop Computers, Smart Phones, or Tablet Devices, you should also follow the *Cyber Security Guideline – End User Computing.*

## 3. Exemptions

3.1. Any exemption or deviation from this Standard must be approved in accordance with the *Cyber Security Standard – Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

| Accountabilities | |
|---|---|
| **Responsible Officer** | Chief Information Security Officer (CISO) |
| **Contact Officer** | Head of Cyber Security Strategy & Governance |
| **Supporting Information** | |
| **Legislative Compliance** | This Standard supports UNSW's compliance with the following legislation:<br>• *Copyright Act 1968* (Cth)<br>• *Corporations Act 2001* (Cth)<br>• *Government Information (Public Access) Act 2009* (NSW)<br>• *Health Records and Information Privacy Act 2002* (NSW)<br>• *Privacy and Personal Information Protection Act 1998* (NSW)<br>• *Public Interest Disclosures Act 1994* (NSW)<br>• *Spam Act 2003* (Cth)<br>• *State Records Act 1998* (NSW)<br>• *Workplace Surveillance Act 2005* (NSW)<br>as well as laws relating to (but is not limited to) breach of confidence, defamation, contempt of court, harassment, vilification and discrimination, the creation of contractual obligations and civil and criminal offenses. |
| **Parent Document (Policy)** | Acceptable Use of Information Resources Policy |
| **Supporting Documents** | Cyber Security Policy<br>Cyber Security Standard – Data Security<br>Cyber Security Standard – Access Control<br>Cyber Security Standard – Information Asset Management<br>Cyber Security Standard – Risk Management<br>Cyber Security Standard – Secure by Design<br>Cyber Security Guideline – End User Computing<br>Cyber Security Standard – Threat and Vulnerability Management |
| **Related Documents** | Data Governance Policy<br>Data Classification Standard |
| **Superseded Documents** | ITSS_13 IT Security Standard - Bring Your Own Device "BYOD" |
| **File Number** | [For Governance Use] |

| Definitions and Acronyms | |
|---|---|
| **Area of Accountability** | Any area where a person has strategic, structural, operational, or financial control over any Information resources within that area. |
| **Digital information** | Means information that is in a digital or electronic form and is stored, processed or transmitted within an Information Service or Information Asset. |
| **Device or Information Asset** | Means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that is stores, processes or transmits UNSW digital information. |
| **EDR (End-point Detection and Response)** | Means endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. |
| **Information Asset** | Means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that is owned by UNSW or provided by UNSW to users. |
| **Information Asset Owner** | Means the person who is accountable for the day-to-day operation and protection of a UNSW Information Asset. |
| **Information Resource** | Means any Information Service, Information Asset, or digital information. |
| **Information Service** | Means any business or technology function using one or more Information Assets including but not limited to: (a) application systems (including software-as-a-service); and (b) IT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services. |
| **Information Service Owner** | Means the person responsible for defining, operating, measuring, and improving a UNSW Information Service and associated cyber security controls. Also known as "System Owner". |
| **Personal Device/Bring your Own Device (BYOD)** | Means a non-UNSW owned or provided device that is used by an individual to access, store, process or transmit UNSW data or digital information. This includes desktops and laptop computers, personal digital assistants, tablets, smartphones, mobile PIN pads, radio communication devices, USB keys or any form of portable storage device. |
| **UNSW Digital Information** | Means digital information that is owned by UNSW. |
| **UNSW Information Asset** | Means any Information Asset that is owned, leased, operated, or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users. |
| **UNSW Information Resource** | Means any Information Resource that is owned, leased, operated, or provided by any UNSW unit or partner to users. |
| **UNSW Information Service** | Means any Information Service that is owned, leased, operated, or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users. |
| **UNSW Owned Device** | Device, which is owned, leased, or provided by any UNSW unit or partner to users. |
| **UNSWIT Managed Device** | An Information Asset that is managed and/or centrally monitored by UNSWIT. |

## Revision History

| Version | Approved by | Approval date | Effective date | Sections modified |
|---|---|---|---|---|
| #.# | [to be completed] | [to be completed] | [to be completed] | [to be completed] |