Purpose

Bring Your Own Device, (“BYOD”) programs are becoming increasingly popular as they give employees the opportunity to choose and purchase their own IT equipment, for both business and personal use. This document defines recommendations and requirements of use, when connecting personally owned devices to the UNSW network.

UNSW supports BYOD, allowing staff and students to purchase personal mobile computing device(s) of their choice and access UNSW’s IT systems. This document applies to, but is not limited to the following devices:

- Smart phones.
- Tablet computers.
- Notebook computers.
- Laptop computers.
- Portable storage devices.

Given the changing landscape of BYO technologies, UNSW must be aware of any new devices that could be used to connect to UNSW network. BYOD devices pose a risk to UNSW information technology systems if not properly managed and should be controlled by the owner in accordance with the recommendations described in this document.

Scope

This document applies to all users including (but not limited to) staff (including casuals), consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to the UNSW.
1.2 Bring Your Own Device - Smart Phone or Tablet Devices (Guidelines)

Remember your smartphone or tablet device is a computer, therefore best practises to protect your personal, UNSW and business sensitive information should be employed.

1.2.1 Ensure operating system and installed “Apps” software, is up to date to protect against known vulnerabilities.

1.2.2 Configure a passcode to gain access to your device to protect against unauthorised access.

1.2.3 Install a secure safe or password manager to store your usernames, passwords and other confidential information.

1.2.4 Leverage device bio-metric access controls if available.

1.2.5 Set an idle timeout that will automatically lock the device when not in use. This also helps prevent unauthorised access.

1.2.6 Install industry standard security solution software, featuring anti-virus, firewall and threat intelligence capabilities.

1.2.7 Run regular virus scans and resolve issues.

1.2.8 Only obtain “Apps” from trusted sources such as “Apple ITunes Store” or “Amazon App Store”. To prevent against malware that may be distributed via untrusted channels.

1.2.9 Do not “jailbreak” or “root” your device as it removes the manufacturer’s protection against malware.

1.2.10 Perform regular data backups to ensure your information is available, should your device be lost, stolen, broken or data corrupted.

1.2.11 Only store UNSW sensitive information on your device if absolutely necessary, i.e. justified academic, research or business need. Ensure sensitive information is encrypted.

1.2.12 If you store sensitive information on your device ensure it is securely removed or transferred to a secure location when no longer required.

1.2.13 If you share your device with friends or family, restrict access to UNSW sensitive information stored on your device.

1.2.14 Enrol your device in a “Find My Phone” service to locate and wipe your device if lost or stolen.

1.2.15 Record the details of your phone in case of theft. Every phone and cellular tablet has a unique International Mobile Station Equipment Identify (IMEI). Most phones allow you to find your IMEI by keying in *#06#. Knowing this number will help your provider stop your phone from being used if stolen.

1.2.16 Label your device with your name and phone number, so it can be returned if stolen even if the battery is dead.

1.2.17 In the event a device containing UNSW information is lost or stolen, report the incident to your local IT Support unit or the UNSW IT Service Desk on (02) 9385 1333 or email servicedesk@unsw.edu.au.

1.2.18 When you recycle your phone, make sure you delete all resident UNSW information and reset the device to factory settings.

1.2.19 Employ reasonable physical security measures when traveling with your device or when at UNSW.
1.3 Bring Your Own Device - Notebook or Laptop Computers (Guidelines)

1.3.1 Ensure all operating system, firmware and application security patches have been applied, to protect against known vulnerabilities.

1.3.2 Configure your device with a strong password or phase phrase.

1.3.3 Install a secure safe or password manager to store your usernames, passwords and other confidential information.

1.3.4 Leverage device bio-metric access controls if available.

1.3.5 Set an idle timeout that will automatically lock the device when not in use. This also helps prevent unauthorised access.

1.3.6 Install industry standard security solution software, featuring anti-virus, firewall and threat intelligence capabilities. UNSW IT has made Symantec End Point software available to all staff and employees. 
https://www.it.unsw.edu.au/students/software/sav.html

1.3.7 Run regular virus scans and resolve issues.

1.3.8 Only obtain applications from trusted sources, to prevent against malware that may be distributed via untrusted channels.

1.3.9 Perform regular data backups to ensure your information is available, should your device be lost, stolen, broken or data corrupted.

1.3.10 Only store UNSW sensitive information on your device if absolutely necessary, i.e. justified academic, research or business need. Ensure sensitive information is encrypted.

1.3.11 If you store sensitive information on your device ensure it is securely removed or transferred to a secure location when no longer required.

1.3.12 If you share your device with friends or family, restrict access to UNSW sensitive information stored on your device.

1.3.13 Label your device with your name and phone number, so it can be returned if stolen or lost even if the battery is dead.

1.3.14 In the event a device containing UNSW information is lost or stolen, report the incident to your local IT Support unit or the UNSW IT Service Desk on (02) 9385 1333 or email servicedesk@unsw.edu.au.

1.3.15 When you recycle your device, make sure you delete all resident UNSW information.

1.3.16 Employ reasonable physical security measures when traveling with your device or when at UNSW.

1.4 Portable Storage Devices and Cloud Storage Solutions (Guidelines)

1.4.1 Perform an anti-virus scan of all portable (USB) media before executing files.

1.4.2 Only store UNSW sensitive information on your device or in the cloud if absolutely necessary, i.e. justified academic, research or business need. Ensure sensitive information is encrypted.

1.4.3 If you store sensitive information on your device or in the cloud ensure it is securely removed or transferred to a secure location when no longer required.

1.5 Access to the Wi-Fi, Bluetooth and Wired networks (Standards / Guidelines)

UNSW allows owners of BYOD to connect to UNSW’s wireless network (uniwide) to access UNSW systems and the internet. The following controls are considered mandatory.

Standards

1.5.1 Access must be authenticated (e.g., 802.1x certificate or username / password) before connecting to UNSW network.
1.5.2 The security logs created by the wireless must be managed according to the ITSS_06 Logging and Monitoring Standard.

1.5.3 Individuals must abide by the rules for use as described in the ITSS_19 IT Acceptable Use Standard at all times.

Guidelines

1.5.4 Only enable Bluetooth when required to mitigate the risk of malicious activity.

1.5.5 Avoid devices running versions of Bluetooth prior to V4, as these are more susceptible to vulnerability.

2. Control Exceptions

All exemption (standard requirements only) requests must be reviewed assessed, and approved by the relevant business stakeholder. Please refer to the ISMS Base Document for more detail.

3. ISMS Mapping with Industry Standards


<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2 Mobile devices and Teleworking</td>
<td>Working Off-Site</td>
</tr>
</tbody>
</table>

4. Document Review, Approval & History

This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the ISSG recommending the formal UNSW policy consultation and approval process commence.

A review of this standard will be managed by the Chief Digital Officer on an annual basis.

4.1 Quality Assurance

This document was designed and created by external and internal consultants in consultation with internal key technical subject matter experts, business and academic stakeholders.

4.2 Sign Off

<table>
<thead>
<tr>
<th>Endorsement</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSG - Information Security Steering Group</td>
<td>30\textsuperscript{th} July 2015</td>
</tr>
<tr>
<td>ITC - Information Technology Committee</td>
<td>27\textsuperscript{nd} August 2015</td>
</tr>
<tr>
<td>CDO – Chief Digital Officer</td>
<td>7\textsuperscript{th} June 2016</td>
</tr>
</tbody>
</table>

Accountabilities

<table>
<thead>
<tr>
<th>Responsible Officer</th>
<th>Chief Digital Officer</th>
</tr>
</thead>
</table>

Contact Officer

ITpolicy@unsw.edu.au

Supporting Information

Parent Document (Policy) | IT Security Policy
Supporting Documents | Nil
Related Documents

Data Classification Standard
Data Handling Guidelines
ISMS Base Document
ITSS_06 Logging and Monitoring Standard
ITSS_19 IT Acceptable Use Standard
<table>
<thead>
<tr>
<th>Superseded Documents</th>
<th>Nil</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNSW Statute and / or Regulation</td>
<td>Nil</td>
</tr>
<tr>
<td>Relevant State / Federal Legislation</td>
<td>Nil</td>
</tr>
<tr>
<td>File Number</td>
<td>2016/16925 [ITSS_13]</td>
</tr>
</tbody>
</table>

### Definitions and Acronyms

No terms have been defined

### Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved by</th>
<th>Approval date</th>
<th>Effective date</th>
<th>Sections modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Vice-President, Finance and Operations</td>
<td>7 June 2016</td>
<td>7 June 2016</td>
<td>This is a new document</td>
</tr>
</tbody>
</table>