End user computing (EUC) Hardware (e.g. desktop, notebooks workstations or tablets) are the primary gateway to the organisation’s sensitive information and business applications. Implementation of appropriate information security controls for EUC hardware can mitigate the risk to UNSW data and IT systems. Consequently end user protection is critical to ensuring a robust, reliable and secure UNSW IT environment.

The purpose of this standard is to set out the rules for effective security measures enforced on EUC hardware as well as any future potential requirements for portable storage and mobile device management.

This standard applies to all users of UNSW Information and Communication Technology resources – including (but not limited to) staff (including casuals), students, consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to UNSW.

The Standard recognises the various types of user SOE (Standard Operating Environment) and non SOE builds deployed throughout UNSW. As such the depth of control that can be applied will differ depending on the level of management in place verses the end user functionality, which must be considered from a risk perspective to achieve a balance.

<table>
<thead>
<tr>
<th>Build Type</th>
<th>Owner / Managed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOE</td>
<td>UNSW IT</td>
</tr>
<tr>
<td>SOE</td>
<td>Faculty IT</td>
</tr>
<tr>
<td>Non-SOE</td>
<td>Research, School, Institute</td>
</tr>
<tr>
<td>Non-SOE (BYOD)</td>
<td>Individual</td>
</tr>
</tbody>
</table>

Note: BYOD devices are primarily applicable to the ITSS_13 BYOD Guidelines.

Are Local Documents on this subject permitted? ☐ Yes ☐ Yes, subject to any areas specifically restricted within this Document ☐ No

Standard

1. Controls..........................................................................................................................2
   1.1 Operating system level security .................................................................2
   1.2 Application level security .................................................................2
   1.3 Logging and monitoring .................................................................2
   1.4 Computing security .................................................................2
   1.5 Mobile / Portable computing security.............................................3
2. Control Exceptions.................................................................................................3
3. ISMS Mapping with Industry Standards ..............................................................3
4. Document Review, Approval & History.................................................................3
   4.1 Quality Assurance..................................................................................3
   4.2 Sign Off.................................................................................................3
1. Controls

1.1 Operating system level security

1.1.1 Security updates and patches must be applied to harden EUC hardware from security vulnerabilities. Patches must be implemented for all EUC hardware by responding to the vulnerability via locally developed process.

1.1.2 Anti-Virus software must be installed and be up-to-date on all EUC hardware. Where the Anti-Virus product provides firewall and intrusion detection capability or any other advanced protection mechanisms this must be considered and enabled where practical.

1.1.3 Anti-Virus products or operating systems must be capable and configured to notify the user when a new program is executed and request user validation.

1.1.4 Where practical, computer access must be managed by a central authentication, authorisation & accounting Service (e.g. Active Directory). This ensures effective and efficient access management.

1.1.5 Access rights (permissions) to modify operating system security parameters such as event logging, password and account management settings must be granted on a justifiable academic or business need basis.

1.1.6 “Local Administrator” access must be granted on a justifiable business need basis.

1.2 Application level security

1.2.1 End users permission to modify the settings of security software (e.g. Anti-Virus) running on desktop and notebook computer must be granted on a justifiable academic or business need basis as directed by the owner.

1.2.2 Application security patches for critical applications such as Microsoft Office, Adobe must be applied in response to the ITSS_04 Vulnerability Management Standard via a locally developed process.

1.2.3 Solutions (Technology & Process) to mitigate the risk of unauthorised applications or code running on end user’s desktop, workstation or notebook must be considered on a risk basis. For example: the benefits of a centrally managed “white listing” solution.

1.2.4 In the absence of requirement “2.2.3” owners must develop a process to ensure only authorised applications or code is installed. The process should be developed from a risk perspective and could empower certain members of the user community the authority to self-approve with the appropriate justification.

1.2.5 Downloading third-party applications onto UNSW owned EUC hardware is only permissible if there is a legitimate academic or business requirement.

1.3 Logging and monitoring

1.3.1 All UNSW EUC Hardware must be configured to capture security event logs according to the ITSS_06 Logging and Monitoring Standard.

1.4 Computing security

1.4.1 Solutions (Technology & Process) to mitigate the risk of sensitive data leakage must be considered on a risk basis. For example: hard disk encryption, secure container, software encryption to ensure confidentiality.

1.4.2 All UNSW EUC Hardware must be subject to inventorying as per the ITSS_08 IT Asset Management Standard.

1.4.3 Solutions (Technology & Process) to mitigate the risk of malicious code infection from the insertion of portable media into EUC Hardware must be considered on a risk basis. For example: anti-virus software with a capability to effectively and efficiently scan portable media.

1.4.4 Ensure UNSW data is wiped, prior to disposal of damaged, upgraded or transferred computing and portable devices, before return to the business owner.
1.4.5 Owners or engaged third party must wipe data from retired or damaged computing and portable devices using secure disposal methods according to the Data Handling Guidelines.

1.4.6 All UNSW EUC hardware must be returned to owners immediately upon employee termination or completion of grant term as per local process.

1.5 Mobile / Portable computing security

1.5.1 Staff must be made aware of the need to secure unattended mobile and portable EUC Hardware (e.g. notebooks, portable hard drives, USB memory sticks etc.) when not in use if the risk is perceived to be high. For example: communal areas such as libraries.

1.5.2 Staff who travel overseas must be made aware of the need to scan mobile (e.g. notebooks) and portable (e.g. portable hard drives, USB memory sticks etc.) EUC Hardware upon return before attaching to the UNSW Network.

1.5.3 Firewall software must be installed and activated on all notebooks.

1.5.4 All UNSW portable EUC Hardware must be returned to UNSW owners immediately upon employee termination or completion of grant term as per local process.

2. Control Exceptions

All exemption 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>Software Security</td>
</tr>
<tr>
<td>12 Operations Security</td>
<td></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>30th July 2015</td>
</tr>
<tr>
<td>ITC - Information Technology Committee</td>
<td>27th August 2015</td>
</tr>
<tr>
<td>CDO – Chief Digital Officer</td>
<td>7th June 2016</td>
</tr>
</tbody>
</table>

Accountabilities

<table>
<thead>
<tr>
<th>Responsible Officer</th>
<th>Chief Digital Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Officer</td>
<td><a href="mailto:ITpolicy@unsw.edu.au">ITpolicy@unsw.edu.au</a></td>
</tr>
</tbody>
</table>
### Supporting Information

<table>
<thead>
<tr>
<th>Parent Document (Policy)</th>
<th>IT Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting Documents</td>
<td>Nil</td>
</tr>
</tbody>
</table>
| Related Documents       | Data Classification Standard  
Data Handling Guidelines  
ISMS Base Document  
ITSS_04 Vulnerability Management Standard  
ITSS_06 Logging and Monitoring Standards  
ITSS_08 IT Asset Management Standard  
ITSS_13 BYOD Guidelines |
| Superseded Documents    | Nil               |
| UNSW Statute and / or Regulation | Nil |
| Relevant State / Federal Legislation | Nil |
| File Number             | 2016/16925 [ITSS_14] |

### 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>