Standard Statement

Purpose
Human Resources Security is one of the most important elements contributing to the overall security of UNSW information. The Security of UNSW information is the responsibility of all staff and students. Furthermore, information security expectations must be clearly defined and communicated to all staff. The purpose of this standard is to set rules that apply before, during and after the termination of employment of all UNSW employees.

Scope
This standard applies to all users of UNSW Information and Communication Technology; resources, including (but not limited to) staff (including casuals), consultants, contractors and students.

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

Standard

1. Controls ..................................................................................................................................... 1
   1.1 Prior to Employment ..................................................................................................... 1
   1.2 During Employment / Enrolment ................................................................................... 1
   1.3 Termination or Change of Employment ........................................................................ 2
2. Control Exceptions.................................................................................................................... 2
3. ISMS Mapping with Industry Standards ................................................................................... 2
4. Document Review, Approval & History ..................................................................................... 2
   4.1 Quality Assurance ......................................................................................................... 2
   4.2 Sign Off ......................................................................................................................... 2

1. Controls

1.1 Prior to Employment

1.1.1 A pre-employment screening process must be undertaken by the University prior to offering employment, to a new employee. Checks must include at least the following:
   • Identity checks (driver’s license, passport, bank account in the same name as the employee, etc.)
   • Reference checks
   • Confirmation of academic or professional qualifications as appropriate
   • Criminal records checks for senior positions

   If the employee is being hired through a third party or staffing agency, screening checks in line with those stated above must be implemented by that agency.

1.1.2 Information gathered on potential employees must be secured by all applicable laws and regulations. Access must be limited to 'need to know' basis.

1.1.3 All staff must agree to comply with UNSW IT Security Policy and Standards prior to being granted access to UNSW Information, Communication and Technology systems. Also, staff may be required to sign a Non-Disclosure Agreement if their role requires access to sensitive information.

1.2 During Employment / Enrolment

1.2.1 UNSW IT must create and deliver a security awareness program promoting the importance of security to all employees and students.

1.2.2 The information security awareness program must be created in two distinct parts:
   • General information security awareness.
   • Information security policy and standards awareness.
1.2.3 Records of awareness campaigns must be kept detailing the type of information security awareness delivered.

1.2.4 Non-compliance with the IT Security Policy and Standards may result in disciplinary action, consistent with the University’s disciplinary processes and procedures.

1.3 Termination or Change of Employment

1.3.1 An employee’s manager must immediately notify the University via an appropriate process upon the resignation or termination of any employee.

1.3.2 Access rights of employees are appropriately modified upon change or termination of employment according to the ITSS_05 User Access Management Standard.

1.3.3 User access rights are reviewed whenever an employee changes roles within UNSW. Management is accountable for the review. The review includes cancelling access rights that are no longer needed unless it has been explicitly authorised by the information system owner or authorised delegates.

1.3.4 Upon termination of employment, the employee’s access rights must be removed from all systems. All IT assets such as EUC Hardware, keys, ID and physical access cards, software, data, and documentation, manuals must be returned to employee’s Manager. Managers are responsible for returning all UNSW IT assets to UNSW IT.

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>7 Human Resources Security</td>
<td>N/A</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>Contact Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Digital Officer</td>
<td><a href="mailto:ITpolicy@unsw.edu.au">ITpolicy@unsw.edu.au</a></td>
</tr>
<tr>
<td><strong>Supporting Information</strong></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---</td>
</tr>
<tr>
<td><strong>Parent Document (Policy)</strong></td>
<td>IT Security Policy</td>
</tr>
<tr>
<td><strong>Supporting Documents</strong></td>
<td>Nil</td>
</tr>
</tbody>
</table>
| **Related Documents** | Data Classification Standard  
Data Handling Guidelines  
ISMS Base Document  
ITSS_05 User Access Management Standard |
| **Superseded Documents** | Nil |
| **UNSW Statute and / or Regulation** | Nil |
| **Relevant State / Federal Legislation** | Nil |
| **File Number** | 2016/16925 [ITSS_18] |
| **Definitions and Acronyms** | No terms have been defined |
| **Revision History** |  |
| **Version** | **Approved by** | **Approval date** | **Effective date** | **Sections modified** |
| 1.0 | Vice-President, Finance and Operations | 7 June 2016 | 7 June 2016 | This is a new document |