UNSW Australia (UNSW) both embraces and relies on the use of technology, the Internet and digital media to conduct academic services. UNSW expects all users who have access to UNSW’s information systems and services to adhere to UNSW rules regarding their use.

The purpose of this standard is to set out the rules for acceptable use of UNSW information systems and services for individuals that have been authorised to use or access the UNSW information systems.

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.

In this Standard, ‘User’ means and includes all staff, students, clinical and adjunct title holders, alumni and other users who are authorised by the University to access its systems and/or network.

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

1. Controls

1.1 Social Media

Social networking media including Facebook, Twitter, wikis, blogs, YouTube and LinkedIn can be useful workplace and academic resources. All users are required to act responsibly when using these sites and comply with the ITSS_19 IT Acceptable Use Standard, Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy and the Social Media Policy of UNSW.

1.1.2 When accessing or contributing on social media sites:

a) Do not place comments representing or giving the impression of representing UNSW unless explicitly authorised to do so.

b) Do not post or view material that is illegal, obscene, defamatory, threatening, harassing, discriminatory, racist or hateful to another person or entity.

c) Be aware that information hosted on social media is unverified and must not be used without confirming its authenticity for decision making.
1.2 Email and Internet Security

1.2.1 Each user is responsible for any digital content that they store on their UNSW devices or sent over UNSW e-mail or Internet services. No communications (including e-mail) may be sent which intentionally hides the identity of the sender or represents the sender as someone else or claims authority of representing someone on their behalf unless explicitly authorised.

You must:

- Contact the UNSW IT Service Desk without delay, if you receive digital information you are not authorised to receive or the information appears illegal or otherwise questionable

You must not:

- Create / send email under another’s name (forgery).
- Create / send / forward: electronic chain letters, unsolicited broadcast emails (“Spam”), obscene, abusive, fraudulent, threatening or repetitive messages.
- Open web links or instructions provided by email, unless you are certain of their origin and function.
- Send any messages that support illegal or unethical activities.
- Change the UNSW security settings of your email client and browser.
- Download any obscene digital material or pornography.
- Download large files without permission (“hogging” bandwidth).
- Attempt to compromise the security of any computer.
- Send emails containing passwords in clear text.

1.2.2 It is acknowledged that despite UNSW’s efforts to the contrary, ICT users may be subject to unendorsed content such as Phishing, Malware and/or other illicit/malicious links or files. It is often the case that such content will utilise social engineering methods to encourage users to unwillingly provide malicious actors access to ICT resources or provide the malicious actors with information such as User Login IDs, Passwords and/or other Personal Identifiable Information, often via the use of fake or misleading websites.

UNSW will endeavor to deploy appropriate security controls and procedures to protect users of ICT services from known Malware, Viruses, Phishing or illicit/malicious content where feasible and deemed appropriate by university policy.

Due to the rapidly changing nature of Malware, Viruses, Phishing or illicit/malicious content, UNSW cannot guarantee protection from all such content. Each user is responsible for applying due diligence and care in the use of ICT services. The University will provide appropriate support and guidance and require the following:

You must:

- Attend Security Awareness training (online or in person) and complete and keep current any associated assessment, as requested by the university.
- Seek advice if you have any IT Security questions or have concerns. Specific contact information can be found on the UNSW Intranet, Local faculty management, Line management or UNSW IT Service Desk on (02) 9385 1333.
- Report a suspected malicious or suspicious email or UNSW web site as a security incident immediately to the UNSW IT Service Desk. See 1.5 Security Incidents.

You must not:

- Open a suspicious email link (links should always end with “.unsw.edu.au” or “.adfa.edu.au”). If you have a concern report it.
b) Open a website or application claiming to belong to UNSW if you are unsure of its authenticity (Phishing schemes often impersonate an official website to trick a user into revealing their login credentials). If you have a concern report it.

c) Open a UNSW website or application that does not have a University domain name (domain names e.g. “website.unsw.edu.au” should always end with “.unsw.edu.au” or “.adfa.edu.au”). If you have a concern report it.

d) Open and enter your user name, password, credentials or personal information into any link (website) that you receive in email, regardless of who they claim to be. **UNSW WILL NEVER** send users links to forms requiring them to:

- Change your password (e.g. Click email link to fix issue)
- Validate your details (e.g. Confirm your Date of Birth)
- Update User information (e.g. Provide your Home Address)
- Log in to fix a full mailbox quota (e.g. Click email link to fix issue)
- Log in to validate your email account (e.g. Click email link to fix issue)
- Log in to fix a problem with email account (e.g. Click email link to fix issue)

*It is also extremely unlikely that other organisations such as Banks, Motor Registry Authorities, Police, Post Office, Council, Utilities (such as Telecommunication, Gas, Electric etc) would ever send such a request. You are encouraged to distrust such requests and contact the organisation directly.*

1.2.3 It is acknowledged that access to potentially unlawful or inappropriate material may be required for legitimate research and teaching purposes. However, access to the following material remains inappropriate UNLESS it has been authorised in writing by a Head of School (or equivalent) as legitimately required for teaching and/or research purposes (including Ethics approval where appropriate) AND access to the material is restricted to legitimate users:

- Access to gambling sites or material that is obscene, pornographic, paedophilic, discriminatory or that promotes illegal acts, or that advocates violence.
- Use of ICT resources to obtain, store, display, copy or transmit potentially unlawful or obscene material.
- Under no circumstances may UNSW ICT resources be used for, or in relation to, corrupt conduct, unauthorised personal financial or commercial gain, or for the unauthorised financial or commercial gain of a third party. Academic staff are referred to the UNSW Paid Outside Work by Academic Staff Policy and general staff to the UNSW Code of Conduct.

1.3 Limited Incidental Personal Use

1.3.1 While UNSW ICT resources are provided for the purposes of business, teaching, learning, and research activities, limited incidental personal use is allowed, so long as such use:

- Is lawful and compliant with UNSW policies and external legislation.
- Does not negatively impact upon the user’s work performance.
- Does not hinder the work of others or interfere with the normal operations of the network.
- Does not damage the reputation or operations of UNSW.
- Does not impose unreasonable or excessive additional costs on UNSW.

Examples of acceptable limited incidental personal use include: an online personal banking transaction; an online airline schedule enquiry or booking.

1.4 Copyright and Intellectual Property

1.4.1 UNSW users must not store, transmit or make available unauthorised copies of copyrighted material using any UNSW end user computing hardware, networks or storage media nor use peer to peer file transfer services or take actions likely to promote or lead to copyright infringement. Users of University ICT resources are responsible for complying with the Copyright law (refer to the UNSW Copyright Ownership Guidelines).
1.4.2 All users obtaining access to other organisations or individuals’ materials must respect all copyrights and must not copy, retrieve, modify or forward copyrighted materials, except with the permission of the copyright owner, or as may be permitted under the appropriate law.

When using UNSW or own devices, networks or storage media you must:

a) Only use licensed software officially installed/registered as owned by UNSW.

b) Only use the applications to which you have authorised access.

c) Comply with the terms of any licence signed by UNSW for online databases, software programs, online publisher packages, etc.

d) Ensure copyright material is only copied or used with the permission of the copyright owner, under the terms of a copyright licensing agreement, or as permitted by law.

When using UNSW computers, networks or storage media you must not:

a) Install or use any unauthorised software;

b) Make/use any illegal copies of licensed software;

c) Use software that you suspect to be unlicensed; or

d) Download, copy, store or transmit material such as music, video or movie files without the express permission of the copyright holder or as permitted bylaw.

e) Download unrelated to teaching, learning or research, which incurs significant additional cost to UNSW.

1.4.3 UNSW IT will periodically audit software installations, to ensure compliance. You must respond to any requests by UNSW IT to provide evidence of software licences for any non-standard software loaded on your Desktop or Notebook.

1.5 Security Incidents

Security Incidents are adverse events that pose a threat to UNSW information systems and services. Security incidents can originate from intentional (deliberate actions against an information system) or unintentional actions (human error).

UNSW has established the ITSS_03 Security Incident Management Standard for the timely and effective handling of information security incidents. Examples of potential security incidents include:

- Abnormal computer behaviour which might be caused by a computer virus, malware or worm.
- A non-escorted guest.
- Disclosure of information to unauthorised person(s).
- Identification devices and removable media are lost, passwords are stolen or disclosed.
- Unauthorised access to an information system or physical premise.

You must:

a) Report a suspected security incident immediately to the UNSW IT Service Desk on (02) 9385 1333.

b) Immediately notify UNSW Campus Security on (02) 9385 6666 or UNSW reception on (02) 9385 1000 if you witness or suspect a physical security incident.

You must not:

a) Perform any action (e.g., delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the UNSW IT Service Desk or UNSW IT Security team.

b) Disclose information relevant to security incidents to unauthorised entities.
1.6 **Adherence to the Standard and Policy**

1.6.1 The University takes non-compliance with this Standard seriously and if any user breaches the standards of use it may result in the following:

- **Staff:** The University may take disciplinary action in accordance with applicable Enterprise Agreements - in serious cases, this may include termination of employment.
- **Students:** The University may deal with non-compliance in accordance with applicable policies and procedures. This may include the University levying fines against non-complying students or taking other action. In serious cases this may involve expulsion. See Appendix 2 – Schedule of Student Fines for Misuse of ICT Resources, in the *Acceptable Use of Information and Communication Technology Resources Procedures*.
- **Non-staff members:** may have commensurate action taken against them, which may include termination or non-renewal of their appointment or contract. Use of, or access to ICT resources may also be restricted or removed.

1.6.2 If UNSW becomes aware of any criminal conduct or an alleged breach of any Australian law, the University may notify the Police or other relevant government authority (e.g. Independent Commission against Corruption).

1.7 **Monitoring Usage of ICT and ICT Resources**

In accordance with the *Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy*, the University will take reasonable precautions to protect the security and privacy of its users’ ICT accounts and ICT Resources. Consistent with these purposes, UNSW will normally only access an employee’s records in the following circumstances:

- When an employee is unexpectedly absent from work (for example, on sick leave or annual leave) and access is required for legitimate business purposes (for example, work continuity) or work health and safety reasons (for example, where there are reasonable concerns about the individual’s health and safety).
- When UNSW reasonably suspects that an individual(s) is not complying with this Policy, other UNSW policies or procedures (e.g. Code of Conduct), or legislation.
- For use in legal proceedings or as required by law (e.g. to comply with a Notice to Produce or subpoena).
- For IT security purposes (e.g. to protect networks or data stored on the network).

Consistent with this approach, access to an employee’s records will only be granted with the approval of the Chief Digital Officer and the Director, Human Resources (or their nominee in circumstances of absence). Access to the records will be provided to an appropriately senior person nominated by the Chief Digital Officer and Director, Human Resources.

For more information on the Workplace Surveillance Act (NSW), refer to the *Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy*.

1.8 **Staff exiting procedure**

1.8.1 When an employee leaves the University, supervisors must ensure that all access to UNSW administrative systems, networks, email accounts etc. is removed or amended as appropriate upon the employee’s departure from UNSW.

If there is to be a continuing relationship with the University after exit (e.g. Honorary appointment, Emeriti, alumnus) then appropriate access to ICT resources can be allocated as per the need.

It may be necessary for a supervisor to access work files or email accounts after an employee’s departure from the University in order to preserve continuity of work. In these circumstances, a departing employee will normally be given the opportunity to remove any personal files or email from University computers prior to their departure.

1.9 **Academic Freedom and Freedom of Expression**

UNSW upholds the principles of academic freedom. This right to academic enquiry and freedom of expression is tempered by the rights of others, including privacy; freedom from intimidation, discrimination or harassment; protection of intellectual property and copyright and ownership of data and security of information.

UNSW requires all users of its ICT resources to do so in a legal, ethical and responsible manner, in accordance with this Standard and other UNSW policies and relevant State and Federal legislation.
While UNSW upholds the principles of academic freedom, it will not condone breaches of UNSW policies or external legislative requirements and will cooperate fully with the authorities in any investigations resulting from a breach. Consequences of a breach may include the removal of access rights to the University’s ICT resources, disciplinary proceedings; and in the case of serious and deliberate breach, may result in civil or criminal proceedings.

For more information on the conditions of use, refer to Section 3.5, Breaching the conditions of use, in the Acceptable Use of Information and Communication Technology Resources Procedures.

1.10 Responsibilities

1.10.1 The Chief Digital Officer has the responsibility for coordinating the implementation of this Standard.

1.10.2 Notifying violations:

Staff and students who become aware of possible violations of this policy must report them immediately to an appropriate person, such as their supervisor, the system administrator, computer lab manager or Head of School. Alleged serious or repeated breaches must be reported to the Chief Digital Officer. In cases where personal safety may be at risk, unauthorised entry to a computing facility has occurred or, where it is believed necessary to seize material held on a University computer, UNSW Security must be contacted for advice and assistance.

1.10.3 External Requests for Information:

If a request is received from an external organisation for information held on University computers (e.g. copies of emails or other correspondence) it must be passed immediately to the University’s Legal Office for investigation and action.

1.10.4 Penalties associated with violations:

Penalties will depend upon the type and severity of breach. Penalties may range from loss or restriction of access, to formal University disciplinary action (which in serious cases may include termination or expulsion). Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

UNSW reserves the right to limit access to its networks through University owned or other computers and to remove or limit access to material and resources stored on University owned computers.

Formal disciplinary action for students will occur in accordance with Student Misconduct Procedures and may include financial penalties as determined by the Chief Digital Officer (see Appendix 2 – Schedule of Student Fines for Misuse of ICT Resources, in the Acceptable Use of Information and Communication Technology Resources Procedures.).

Formal disciplinary action for staff will occur via the procedures outlined in the relevant industrial instrument (e.g. an applicable enterprise agreement).

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>8 Asset Management (8.1 Responsibility of Assets)</td>
<td>Using the Internet</td>
</tr>
<tr>
<td>13 Communications security (13.2 Information transfer)</td>
<td>Email Security</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>
</tbody>
</table>

Supporting Information

<table>
<thead>
<tr>
<th>Parent Document (Policy)</th>
<th>Supporting Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Policy</td>
<td>Nil</td>
</tr>
</tbody>
</table>

| Related Documents
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy</td>
</tr>
<tr>
<td>Data Classification Standard</td>
</tr>
<tr>
<td>Data Handling Guidelines</td>
</tr>
<tr>
<td>ISMS Base Document</td>
</tr>
<tr>
<td>ITSS_03 Security Incident Management Standard</td>
</tr>
<tr>
<td>Acceptable Use of Information and Communication Technology Resources Procedures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Superseded Documents</th>
<th>UNSW Statute and / or Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil</td>
<td>Nil</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant State / Federal Legislation</th>
<th>File Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil</td>
<td>2016/16925 [ITSS_19]</td>
</tr>
</tbody>
</table>

Definitions and Acronyms

For definitions and information relating to key terms and acronyms referred to in this Policy and IT Security Standards please refer to the [ISMS Glossary](#).

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>
<tr>
<td>1.1</td>
<td>Vice-President, Finance and Operations</td>
<td>27 September 2016</td>
<td>27 September 2016</td>
<td>Section 1.1.1; 1.2.2 (new); 1.5(a); 1.6.1; 1.7; 1.9; 1.10.4; remove Appendix</td>
</tr>
</tbody>
</table>