As an innovative academic institution, UNSW does not restrict itself when considering the engagement of ICT services from external service providers, in the delivery of academic, research and business objectives. The purpose of this Standard is to set out the rules and requirements that must be satisfied when leveraging cloud computing services offered by a Cloud Service Provider (CSP).

UNSW may wish to engage a CSP to:

- Minimise the capital expenditure required to procure and deliver IT and software assets using traditional IT service delivery models.
- Gain access to leading technology, offering enhanced and cost-effective resiliency solution in comparison to an in-house solution.
- Obtain elastic capacity that is flexible and can instantaneously expand to meet unexpected rapid increase in demand of student-facing services.
- Leverage technologies of cloud services for the provisioning of current and future services without additional investment (e.g., hardware/software, personnel capacity/expertise etc).

This standard applies to all users of 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.

Typical cloud-based service information security requirements are:

- Geographical location of deployed services and notification of change requirements.
- Preventing the transfer of sensitive information e.g. Personal Identifiable Information overseas without adequate steps to protect the confidentiality and integrity of information.
- Protecting the information stored from unauthorised access such as other cloud service customers or administrators.
• Preventing access to Personal Identifiable Information (PII) when cloud computing services move information between different physical equipment and storage mechanisms.
• As cloud services provide limited visibility of how the services are delivered, the confidentiality and integrity of information must be sustained and ensured at all levels (e.g., hardware, backups etc.).
• Ensure adequate security contractual controls including auditability controls, physical security controls, logical security controls, ability to extract data (e.g., bring the data in house or move it to another CSP), alignment with international security standards and defined security incident management processes.

1.2 Prior to consuming Cloud services

1.2.1 A risk assessment must be performed to identify the necessary security controls that must be established to manage risks to an acceptable level. The risk assessment must include a gap analysis between (a) UNSW’s IT Security Policy and Standards and (b) the security controls operated by the CSP identifying the threats to UNSW information.

1.2.2 Adequate assurance must be gained that identified risks have been addressed and that the appropriate security controls are in place before sensitive information is transferred to the cloud-based service.

1.2.3 Any UNSW information hosted or processed by the CSP must be classified per the UNSW Data Classification Standard. Importantly this process must identify and document the points where information will be stored, processed and transmitted within the solution. CSP’s must implement the data security controls in accordance with UNSW’s Data Handling Guidelines.

1.2.4 Clarification must be sought on which aspects of the CSP business are covered by ISAE 3402 or other security standards such as ISO27001, Cloud Security Alliance (CSA) and Governance, Risk Management and Compliance (GRC) Stack. Copies of the latest external and internal audit reports must be supplied to UNSW.

1.2.5 Legal advice must be sought with regards to:

• The safeguards required for the use of CSPs involving information that UNSW is legally obliged to protect, such as Personal Information and Research data, in accordance with applicable; Commonwealth, State and Territory privacy laws.
• If information is to be managed offshore the regions jurisdiction over the information must be taken into consideration from a regulatory perspective concerning data privacy and in particular data sovereignty.

1.2.6 Where a multi-tenanted Cloud platform is being considered (e.g., a single instance of a software application serves multiple customers) a procedure must be in place to ensure the suitable segregation of UNSW’s data from other clients of the CSP.

1.2.7 Prior to engaging a CSP appropriate assurance must be sought such that access to UNSW sensitive data by the CSP staff and any third parties is restricted and monitored.

1.2.8 UNSW must ensure that security-related event logs generated as part of the cloud service (at the application, operating system, database and network level) are stored, reviewed and retained by the CSP in accordance with UNSW’s Retention Policies.

1.2.9 The deployment of a Security Information and Event Management (SIEM) solution for automated log consolidation, correlation, alerting and storage, may also need to be requested by UNSW to facilitate effective analysis and management of log data.

1.3 Contracting with Cloud service providers

1.3.1 The CSP must contractually and operationally commit to meeting UNSW security and regulatory compliance requirements. UNSW must confirm and include specific security and regulatory compliance clauses in the contract with the CSP as described in UNSW ITSS_20 Third Party Risk Management Standard.
1.4 During the Cloud services

1.4.1 The performance and effectiveness of the security controls implemented by the CSP must be assured at least annually and executed based on criticality of the service basis. Exceptions must be recorded and remediation activities tracked in accordance with UNSW risk management practises.

Note: The level of inspection very much depends upon what has been agreed via contract, for example requesting copies of the CSP certification may suffice.

1.4.2 Procedures must be in place for the CSP to inform UNSW in the event of a suspected or actual security incident involving a UNSW service or information. Any incidents identified must be handled in accordance with the ITSS_03 Security Incident Management Standard.

1.5 Cloud services availability

In line with IT Recovery ITSS_16 standard these following Business Continuity and Disaster Recovery

1.5.1 Scheduled outages must be included in the contract and SLA’s to avoid disruption of UNSW services. Schedule notification processes for outages and how the disruption will be minimised must be clearly defined.

1.5.2 Disaster recovery processes need to adhere to UNSW policy and recovery commitments need to ensure restoration of services are within reasonable timeframes.

1.5.3 The CSP’s business continuity and disaster recovery plans must be understood to determine how long it will take to restore scoped services, the order in which they will be restored and the priority between customers.

1.5.4 Disaster recovery test results must be communicated by the CSP to UNSW on an annual basis to ensure that scoped service’s recovery remain in line with UNSW business requirements.

1.6 Cloud services termination

1.6.1 Upon termination of cloud services, all UNSW data must be securely returned / transferred to UNSW and removed from CSP information systems and storage media.

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>ISO/IEC 27017</td>
<td>Information Security Engagement (Industry Engagement and Outsourcing)</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**

- **Responsible Officer**: Chief Digital Officer
- **Contact Officer**: ITpolicy@unsw.edu.au

**Supporting Information**

- **Parent Document (Policy)**: IT Security Policy
- **SupportingDocuments**: Nil
- **Superseded Documents**: Nil
- **UNSW Statute and / or Regulation**: Nil
- **Relevant State / Federal Legislation**: Nil
- **File Number**: 2016/16925 [ITSS_07]

**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>