ITSS_20   IT Security Standard – Third Party Risk Management

Standard Statement

Purpose
UNSW must ensure that contracted third parties apply equally stringent controls in managing and protecting UNSW sensitive data. As such, adequate contracts and due diligence processes protecting UNSW must be in place.

Scope
This standard will set out the basic rules for managing the security over third parties (i.e., suppliers, vendors etc) who maintain direct or indirect access to UNSW IT systems and data. This standard applies to all third parties including corporations, individuals, sub-contractors or parties engaged by any external service provider with whom UNSW has a commercial relationship with for the provision of IT services and who may be handling or have access to UNSW information.

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

1. Controls....................................................................................................................................... 1
1.1 Third party selection and evaluation process ............................................................................. 1
1.2 Contracting with third parties ...................................................................................................... 2
1.3 Ongoing third party risk management ........................................................................................ 3
2. Control Exceptions...................................................................................................................... 3
3. ISMS Mapping with Industry Standards ..................................................................................... 3
4. Document Review, Approval & History....................................................................................... 4
4.1 Quality Assurance....................................................................................................................... 4
4.2 Sign Off....................................................................................................................................... 4

1. Controls

1.1 Third party selection and evaluation process

1.1.1 A UNSW third party evaluation process must exist to assess external parties that will provide IT services to UNSW. The following elements must be considered during the third party evaluation process:

a) Third party financial status (i.e. annual turnover).

b) The effect of the contract (that will be signed between the two parties) on the third party turnover.

c) Third party reputation and client portfolio.

d) Third party organisational structure, personnel profile/workforce, resumes for all IT professional services, consultative services or other service related engagements and demonstrated domain capability/expertise.

e) Third party insurances and their conformance to UNSW Procurement Policy.

f) Third party Quality Assurance and quality control framework (includes compliance with policies, standards, procedures and guidelines and formal accreditations, for example ISO9001).

g) The ability of the third party to comply with national and international statutory and regulatory requirements e.g. PCI DSS and privacy legislation.

h) The reliability, security and effectiveness of third party IT systems.

i) The completeness of third parties technical support procedures (with respect to the offered services including review of offered SLA and KPI).

j) Third Party business continuity and disaster recovery plans.
1.1.2 UNSW information and information systems will be exposed to risks by allowing access from external party organisations with unknown information security management systems. Where there is a business need to provide external parties access to UNSW information facilities or for them to hold UNSW data, a risk assessment is carried out to identify requirements for specific information security measures.

1.1.3 The risk analysis will take into account the type of access required, the value of the information, the information security measures employed by the external party and the implications of the access for the security of UNSW information and information systems. As part of the risk assessment the UNSW IT Security Questionnaire is completed by third parties providing details around their information security management system and control environment.

1.1.4 Access to UNSW facilities or data by external parties is not provided until the appropriate measures have been implemented and an agreement has been signed defining the terms and conditions for the connection. Refer to ITSS_05 User Access Management Standard for further guidance on security for remote access to a UNSW network.

1.1.5 The UNSW IT team is responsible for performing the risk assessments and evaluating third party’s security control environment.

1.1.6 An external party can demonstrate their information security credentials to UNSW in one of the following ways:

- Certification— if the external party can produce a current certificate showing compliance to the relevant standard, ISO 27001, with a relevant scope, then they may be considered to have complied with this requirement.
- External Audit— if the external party has had their information security policies and practices audited by a trusted and independent organisation, and they are able to deliver a satisfactory report of that audit, then they may be considered to have complied with this requirement.

1.1.7 A third party inventory must exist which describes the services provided along with the criticality of each third party (e.g., High/Medium/Low) based on the results of the risk assessment.

1.1.8 To simplify market engagement and reduce workload in third party management UNSW IT Procurement has pre-qualified a number of third party providers including legal and contractual considerations. IT Procurement can advise on the use of the pre-qualified organisations and use of the pre-agreed contracting structures to reduce third party management overheads. Pre-qualification includes:

a) UNSW Preferred Supplier Arrangements,

b) UNSW IT related Panels, and

c) Other Panels and Schemes pre-qualified by a party recognized by UNSW.

1.1.9 Further information on UNSW preferred supplier arrangements contact IT Procurement or UNSW Buying Guide at http://www.fin.unsw.edu.au/OurServices/Procurement_BuyingGuide.html. For information on both UNSW and other IT related Panels contact IT Procurement (itprocurement@unsw.edu.au).

1.2 Contracting with third parties

1.2.1 Third parties must contractually and operationally commit to meeting UNSW commercial, security and any regulatory compliance obligations. The following requirements must be included in third party agreements:

a) External parties are covered by a non-disclosure agreement that explicitly states that persons with access to UNSW facilities or proprietary information are not to disseminate any information about UNSW, its capabilities or activities without written authorisation from UNSW.

b) The obligation of the third party to notify UNSW in cases of security incidents occurring within the third party, which may affect UNSW (e.g. third party virus outbreak, successful third party network compromise etc).

c) The obligation of the third party to maintain confidentiality integrity and availability of UNSW information.
d) The possibility of renegotiating or terminating the contract if the terms and conditions are not satisfied, for example an undisclosed security incident or third party failing to meet agreed service levels.

e) Sub-contracting issues in case the third parties (e.g. Cloud Service Providers) make use of other suppliers for the delivery of the services and these suppliers maintain direct or indirect access to UNSW's data. The third party must commit that any suppliers meet UNSW security and regulatory compliance obligations.

f) All outsourcing contracts must include an agreement on acceptable security controls and a requirement that the outsourcer provide an ISAE 3402 or equivalent document (e.g., ISO27001 certification) on an annual basis.

g) Controls must be in place to ensure the security of remote connections between the parties. The third party must utilise the existing UNSW security infrastructure and take responsibility for the maintenance of the respective security controls that have been established by UNSW.

h) The third party must ensure that any suppliers they utilise to fulfil contract requirements meet UNSW security and regulatory compliance obligations.

i) Ownership of licensing and intellectual property, including escrow agreements must be clearly defined.

j) To the extent possible, a "right to Audit" clause ensuring that management and / or an authorised representative may physically and or logically evaluate a third party's control environment.

k) The type, volume and frequency of any files and/or reports that will be exchanged between the two parties

l) The business continuity and disaster recovery arrangements for the resumption of the third party services in case of service interruption or data loss/destruction.

1.2.2 UNSW Procurement teams (faculty, divisions) or individuals responsible for the selection and approval of third party ITC services where necessary, engage a legal review of contracted information services agreements.

1.2.3 UNSW IT Procurement to base all third party agreements on a template, third party contract. The template, third party contract must be reviewed by the UNSW Security Governance Manager on an annual basis. IT procurement can advise on the use of pre-qualified organisations and use of pre-agreed contracting structures to reduce risk analysis overheads.

1.3 Ongoing third party risk management

1.3.1 All third parties classified as "high risk" must be subject to annual security review by UNSW security team or an authorised representative. The security review must be conducted against the security requirements and respective controls depicted in the UNSW ISMS Policy and Standards.

The results of the annual review must be communicated to the third party and the third party must commit to specific dates for remediating any identified security issues.

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>15 – Supplier Relationships</td>
<td>Information Security Monitoring (Vulnerability Management)</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>30rd July 2015</td>
</tr>
<tr>
<td>ITC - Information Technology Committee</td>
<td>27rd 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>

<table>
<thead>
<tr>
<th>Related Documents</th>
<th>Data Classification Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Handling Guidelines</td>
</tr>
<tr>
<td></td>
<td>ISMS Base Document</td>
</tr>
<tr>
<td></td>
<td>ITSS_05 User Access Management Standard</td>
</tr>
</tbody>
</table>

<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>
</tbody>
</table>

| File Number                  | 2016/16925 [ITSS_20]       |

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>