IT Security Policy – Information Security Management System (ISMS)

Version	Approved by	Approval date	Effective date	Next review date
3.0	President and Vice-Chancellor	7 June 2016	7 June 2016	7 June 2019

Policy Statement	
Purpose	To ensure that UNSW information can be used when required with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorised disclosure, damage or loss. The policy reinforces the value of data and information to UNSW. The IT Security Policy sets out management's information security direction and is the backbone of the UNSW Information Security Management System (ISMS). The purpose of the ISMS is to proactively and actively identify, mitigate, monitor and manage information security vulnerabilities, threats and risks in order to protect UNSW and its assets, information and data. The ISMS sets the intent and establishes the direction and principles for the protection of UNSW's IT assets. This is to enable continuous improvement of UNSW security capability and resilience to emerging and evolving security threats.
Scope	This policy applies to all users of UNSW ICT 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. This applies to all UNSW IT Assets and all devices connected to the UNSW network.
Policy Provisions	

Contents

1. Preamble

The University of New South Wales (UNSW) values the use of information technology in supporting the mission of the University. Our academic services gain strength and currency from our research activities, strong industry links and our international nature. UNSW has strong engagements with partnerships from both local and global communities allowing UNSW to share knowledge, debate and research outcomes.

In this context, UNSW information, whether managed and residing on UNSW resources or held in trust and managed by third parties or business partners, is an important asset that must be protected. Any person or organisation that uses or holds in trust these assets has a responsibility to maintain and safeguard them.

The University is committed to preserving the confidentiality, integrity, and availability of information regardless of the form it takes - electronic or non-electronic. Improper use of information resources may result in harm to the University and its mission of teaching, research, and international outreach.

2. Policy Statements

2.1 Data Backup

Data Backups are primarily a preventative measure to protect against loss of data resulting from system failure (disaster or other), virus/malware attack, system or human error.

Backups are an essential control and safeguard to ensure availability of UNSW information being stored, processed or transmitted via information technology communication systems.

Statement: Data must be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster. See *Data Backup Standard ITSS_01*

2.2 Data Security

UNSW supports an extensively broad and complex data landscape. Based on appropriate data classification and handling guidelines, this policy and associated standard ensures that appropriate controls are implemented for the confidentiality and integrity of sensitive data.

Statement: Encryption techniques must be used for protecting sensitive data during transmission and storage. *See Data Security Standard ITSS_02*

2.3 Security Incident Management

Provides preventive, corrective and detective measures, ensuring a consistent and effective approach to the management of information security incidents, including communication of events and weaknesses, such as breach of access.

Well designed, understood tools and processes will help contain, preserve (legal / forensic purposes) and limit any damage resulting from a security incident.

Statement: Incident detection mechanisms such as security event logging and antivirus must be implemented for all IT systems. All potential security incidents must be handled appropriately following a formalised security incident handling process. *See Security Incident Management Standard ITSS_03*

2.4 Vulnerability Management

All systems are susceptible to vulnerability (weakness) and therefore under constant threat from malicious exploitation that may result in the compromise of confidentiality, integrity or availability of UNSW information or systems, potentially resulting in productivity, reputational or financial loss.

Vulnerability management involves alerting and responding to identified and potential violations or security threats in a timely, measured and prioritised (risk based) manner, in order to prevent or limit the damage. Vulnerability management is considered a preventive and corrective measure.

Statement: Security patch and vulnerability management processes must be in place to identify, prioritise and remediate security vulnerabilities on IT assets. *See Vulnerability Management Standard ITSS_04*

2.5 User Access Management

A preventive measure, ensuring only authorised users are granted access to UNSW systems. Unauthorised access could enable a malicious or accidental security breach.

Breach of access could lead to unwanted release or manipulation (Integrity) of sensitive information potentially resulting in productivity, reputational or financial loss.

Statement: All user access related requests (e.g. adding new users, updating access privileges, and revoking user access rights) must be logged, assessed and approved in accordance with defined user access management process. *See User Access Management Standard ITSS_05*

2.6 Logging and Monitoring

Security devices such as firewall, Intrusion detection / prevention, security event incident management, mail content filters and anti-virus all generate log data.

The timely detection of information security incidents relies on comprehensive security log data being available from information technology communication systems.

Statement: Key security-related events such as user privilege changes must be recorded in logs, protected against unauthorised changes and analysed on a regular basis in order to

identify potential unauthorised activities and facilitate appropriate follow up action. *See Logging and Monitoring Standard ITSS_06*

2.7 Cloud Security

UNSW is increasingly utilising cloud solutions to deliver business solutions and functionality. This Policy and Standard explains what UNSW expects of "cloud service providers" to meet security controls and access requirements to ensure all UNSW information and system controls are met.

This requirement is closely related to "Third Party Risk Management (See 5.20)". Additionally, cloud service providers have been known to change practices with minimal notice. These impacts need to be managed or mitigated in our agreements to meet UNSW service expectations.

Statement: UNSW sponsored and endorsed cloud based services must be consumed following a formalised risk assessment to identify the necessary security controls that must be established by the Cloud Service Provider and UNSW to manage security risks to an acceptable level. *See Cloud Security Standard_ITSS_07* and *Data Handling Guidelines*.

2.8 IT Asset Management

Asset / Inventory management is key to prudent security and management practices, providing context for all IT Security Policy statements and Standard requirements.

Without an accurate inventory, processes such as vulnerability management are difficult to implement. For example, assessment of in scope devices when responding to critical vulnerabilities, may not be captured, hence devices will remain unpatched and therefore exposed to malicious exploit.

Statement: In the context of this policy, an IT asset is any UNSW owned or managed device or service that connects to or is used by UNSW in its business, research, teaching and learning activities such as data link, physical device, application (including firmware), database and middleware. *See IT Asset Management Standard ITSS_08*

Based on Data Classification, Asset Owners must implement appropriate ISMS and Data Handling controls to maintain Confidentiality, Integrity and Availability of UNSW Data.

2.9 Change Management

The UNSW IT Change Management process ensures stability and availability of related information technology communication systems across UNSW. Secure practices including reviews during changes are necessary to ensure service availability.

Statement: Any change to UNSW production information systems must be logged and assessed for security and risk impact as documented in the UNSW Change Management Process. The requirements, risk and impact of each request must be evaluated and the proposed risk mitigation solution must be documented and approved. *See Change Management Standard ITSS_09*

2.10 IT System Acquisition & Development

IT systems (applications, databases & middleware) are susceptible to attack and therefore security controls must be embedded throughout the whole acquisition development lifecycle.

In conjunction with this and other controls, a multi-level approach to information security at each layer of the system must be taken, therefore mitigating the security risk.

Statement: IT security requirements must be addressed within the software development lifecycle, to reduce the risk of vulnerabilities being introduced during the acquisition or development of IT systems. *See IT System Acquisition & Development Standard ITSS_10*

2.11 Web Application Security

Web applications are being used extensively across UNSW for the delivery of business services and information. They also represent one of the highest exposures to security attacks. Given the number of security exploits that exist for web interfaces, secure design, implementation and monitoring are essential.

Statement: Web applications need to be designed, built and tested (verified) to ensure security is applied at all layers of the application and technology. Assessment and design guidelines provide controls to be followed when developing UNSW internet-facing (Web) applications. *See Web Application Security Standard ITSS_11*

2.12 Physical Security

Physical security is important for critical infrastructure that must be protected from physical (theft) or environmental (fire, water) damage. Physical security is very much a preventive control.

Statement: The facilities (e.g., data centres, computer rooms etc.) where critical information is stored or processed, must be constructed and arranged in a way that data is adequately protected from physical and environmental threats. *See Physical Security Standard ITSS_12*

2.13 Bring Your Own Device (BYOD)

Supporting “Bring Your Own Device” provides choice and flexibility for UNSW staff and students. This allows increased personal productivity and improved work experience but also necessitates additional security controls and measures to protect the UNSW information and systems.

This Policy and associated Guideline recognises this need and provides the requirements to manage the risks associated with “BYOD”.

Statement: UNSW staff, students and authorised users connecting personally owned devices to the UNSW networks must comply with secure practices to ensure the security of UNSW networks and UNSW data in their devices. *See Bring Your Own Device Guideline ITSS_13*

2.14 End User Protection

UNSW end user devices are the primary gateway to UNSW’s data and business applications. Implementation of appropriate information security controls is necessary to mitigate the risk of inappropriate access to UNSW data and IT systems such as malware, information disclosure or loss.

Consequently end user protection is critical to ensuring a robust, reliable and secure IT environment. Failing to do so can result in an information security incident, causing financial and/or reputational loss to UNSW.

Statement: End user desktop computers, mobile computers (e.g., laptops, tablets) as well as portable computing devices (e.g. portable hard drives, USB memory sticks etc.) must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of UNSW data. *See End User Protection Standard ITSS_14*

2.15 Network Security

Network infrastructure and associated data links provide essential connectivity between internal and external systems. In order to provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed in line with current security practises.

Statement: UNSW network architecture must commensurate with current and future business requirements as well as with emerging security threats. Appropriate controls must be established to ensure security of UNSW data in private and public networks, and the protection of IT services from unauthorised access. *See Network Security Standard ITSS_15*

2.16 IT Recovery

Service availability is critical for UNSW Information Technology communications, infrastructure, systems and applications. This Policy ensures that processes are in place to ensure UNSW's ability to recover from system and environmental failures, and regular testing of these processes is afforded.

Statement: An IT Recovery Plan and relative process must be in place to enable the recovery of business critical UNSW services in a timely manner, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption. *See IT Recovery Standard ITSS_16*

2.17 Information Security Risk & Compliance Management

Risk Management is at the core of the Information Security Management System. Allowing UNSW to identify, assess and evaluate risk, enabling, effective management of information security vulnerabilities and threats to its information assets that could adversely affect or provide academic and business opportunities.

Statement: Information security risk must be identified, mitigated and monitored through a formalised risk management process.
Compliance with UNSW ISMS must be measured and monitored to ensure that UNSW Divisions and Faculties abide by ISMS's security controls. See *Information Security Risk and Compliance Management Standard ITSS_17*

2.18 Human Resources Security

Supporting Human Resources policies, the purpose of this Policy and Standard is to define the rules to be followed before, during and after the termination of employment of all UNSW employees.

Statement: All UNSW staff (Including casuals), consultants, contractors, third parties, agency staff, associates, honoraries, and conjoint appointments must be subject to appropriate security processes before, during and after the termination of their employment. *See Human Resources Security Standard ITSS_18*

2.19 IT Acceptable Use

UNSW embraces and relies on the use of technology, the Internet and digital media to conduct academic and business activities. This Policy and associated Standards outline the acceptable practices in the use of technology and access to information sources and systems for UNSW system users, and complements the "Acceptable Use of UNSW Information and Communication Resources (ICT) Policy".

Statement: All users who have access to UNSW's IT systems and services must adhere to specific rules regarding use of UNSW resources, their internet and email usage as well as when interacting with social media. *See IT Acceptable Use Standard ITSS_19*

2.20 Third Party Risk Management

Outsourced agreements should enforce appropriate information security controls with respect to the nature of the contract i.e. cloud services engagement, to ensure proper due diligence and therefore risk management.

Statement: Security risks arising from UNSW contracted third parties (i.e., suppliers, vendors etc.) who maintain direct or indirect access to UNSW IT systems and data must be operationally and contractually controlled. *See Third Party Risk Management Standard ITSS_20*

3. Legal & Policy Framework

The IT Security Policy sets the foundation for UNSW compliance with:

- Digital Information Security Policy (NSW) *(https://arp.nsw.gov.au/m2012-15-digital-information-security-policy)*
- State Records Act 1998 (NSW) *(http://www.records.nsw.gov.au/about-us/state-records-act-1998)*
- Privacy & Personal Information Protection Act 1998 (NSW) *(http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/)*
- Health Records & Information Protection Act 2002 (NSW) *(http://www5.austlii.edu.au/au/legis/nsw/consol_act/hraipa2002370/)*
- Government Information Classification and Labelling Guidelines 2013 (NSW) *(http://arp.nsw.gov.au/dfs-c2013-05-information-classification-and-labelling-guidelines)*
- Privacy Amendments (Privacy Alerts) Bill 2013 (Cth) *(http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5059)*
- Privacy Amendment Act 2012 (Cth) (*https://www.comlaw.gov.au/Details/C2012A00197)*
- Australian Government Cloud Computing Strategic Direction 2011 (AGIMO) (*http://www.finance.gov.au/files/2012/04/2011-001_AGIMO_Circular_Cloud_Computing_Strategic_Direction_Paper.pdf)*
- Australian Government Cloud Computing Policy 2013 (AGIMO) *(http://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf)*
- Government Cloud Services Policy and Guidelines (NSW) *(http://www.finance.nsw.gov.au/ict/sites/default/files/NSW%20Government%20Cloud%20Services%20Policy%20and%20Guidelines.pdf)*
- Australian Government Protective Security Policy Framework (PSPF) *(https://www.protectivesecurity.gov.au/Pages/default.aspx)*

This policy is aligned with the following UNSW internal Policies, Guidelines and Frameworks:

- Data Classification Standard
- Data Handling Guidelines
- Digital Media Policy
- Acceptable Use of UNSW Information and Communication Resources (ICT) Policy
- Risk Management Policy
- Record Keeping Policy
- Privacy Policy
- Procurement Policy
- UNSW Code of Conduct

4. Implementation

The implementation of the IT Security Policy will be achieved by performing an assessment of existing IT Security Practices, against the relevant ISMS controls and necessary remediation of any perceived deviations.

4.1 Roles & Responsibilities

Roles and responsibilities are set out in the ISMS Framework Security Roles and Responsibilities document.

4.2 Support & Advice

The contact for support and advice relevant to this Policy is the ITpolicy@unsw.edu.au

5. Review

The IT Security Policy is an active document and must be subject to independent review. Management review must be conducted according to UNSW Governance Support Process.

This Policy will be reviewed by the Chief Digital Officer every three years from the effective date.

6. Acknowledgements

The following sources have been consulted for the development to this policy:

- ISO/IEC FDIS 27001:2013
- COBIT 5 for Information Security
- Australian Government, Department of Defence Information Security Manual

Accountabilities	
Responsible Officer	Vice-President, Finance & Operations
Contact Officer	Chief Digital Officer
Supporting Information	
Supporting Documents	IT Security Standards: ITSS_01 to ITSS_20

Related Documents	Acceptable Use of UNSW Information and Communication Resources (ICT) Policy Data Classification Standard Data Handling Guidelines Digital Media Policy Risk Management Policy Recordkeeping Policy Privacy Policy Procurement Policy UNSW Code of Conduct
Superseded Documents	IT Security Policy, version 2.1 effective 18 February 2010
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2015/36180

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

Version	Approved by	Approval date	Effective date	Sections modified
1.0	VCAC			
2.0	Vice-Chancellor	18 February 2004	1 March 2004	Full review
2.1	Head, Governance Support	18 February 2010	18 February 2010	Sections 3.1, 5, 12
3.0	President & Vice-Chancellor	7 June 2016	7 June 2016	Full review