



THE UNIVERSITY OF  
NEW SOUTH WALES

## *UNSW IT Security Policy*

<b><i>Policy Name:</i></b>	IT Security Policy	<b><i>Contact Officer:</i></b>	Jenny Beatson, Policy Officer, Division of Information Services
<b><i>Approving Authority</i></b>	Vice-Chancellor	<b><i>Date of Approval:</i></b>	February 18 2004
<b><i>Due for Review:</i></b>	February 2005	<b><i>Last Amended:</i></b>	July 1997

UNSW recognises that policies, rules, guidelines and administrative material placed into the public domain of the University's website may be of assistance to other organisations and universities as reference material or models. The University requests that when UNSW material is used in development of documents, the work done by the University is acknowledged by referencing the source of the ideas or written expression. For further information contact Debbie Osborn, Head of Policy Management at [d.osborn@unsw.edu.au](mailto:d.osborn@unsw.edu.au)

## Table of Contents:

1. Introduction .....	3
2. Security principles for UNSW .....	4
2.1 Protection of information .....	4
2.2 Systems Access Controls.....	4
2.3 Access Privileges – (Minimum possible privilege) .....	5
2.4 Remote access .....	5
2.5 Business Risk based controls.....	5
2.6 Classification of UNSW information .....	6
2.7 UNSW Information ownership.....	6
2.8 Security exceptions will be managed .....	7
2.9 Enforceable and Practical Policies.....	7
2.10 Compliance with legal and regulatory obligations .....	8
2.11 Standards acknowledged.....	8
2.12 Inform users of policy.....	8
3. Information Assets, Classification and Responsibility .....	9
3.1 Information Assets and Inventory .....	9
3.2 Information Classification .....	9
3.3 Allocation of Information Security Responsibilities.....	9
3.4 Risk Analysis.....	9
3.5 Security of Third Party Access.....	9
4. System and Information Access Control .....	10
Access policies and procedures.....	10
5. User Education and Responsibilities.....	11
5.1 User's Acceptance of Responsibilities .....	11
5.2 Authentication.....	11
5.3 Unattended Equipment.....	12
5.4 Breaches of Policy.....	12
6. Physical and Environmental Security for Critical and Sensitive Information .....	12
6.1 Facility Security.....	12
6.2 Clear Desk Policy .....	12
6.3 Removal of Property.....	13
6.4 Equipment Security .....	13
7. Computer and Network Management.....	13
7.1 Operational Procedures and Responsibilities .....	13
7.2 Protection from Malicious Software and Viruses .....	13
7.3 Network security controls.....	13
7.4 Electronic mail.....	13
7.5 Internet Use.....	14
8. Security Requirements of IT Systems .....	14
8.1 Business risk analysis.....	14
8.2 Regular security review.....	14
9. Business Continuity Planning .....	15
10. Compliance with Legal Requirements.....	15
10.1 Compliance with IT Security Policy .....	15
10.2 Compliance with legislation .....	15
11. Definition of Terms.....	16
12. Related Documents referenced in the policy.....	18

# ***UNSW IT Security Policy***

In this policy there are three discrete levels of issues related to IT Security. It includes the security principles, the policy statements, and in an associated document, the IT Security standards. The policy statements are the intentions of University management and are based on the security principles.

A separate security standards document provides how-to instructions and guidelines for users.

A series of definitions is included at the end of this document.

## ***1. Introduction***

Information takes many forms. It can be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. Information and Information Technology systems are assets of vital importance to the University of New South Wales; they are central to the daily operation and to the future advancement of the University.

At UNSW, Information security has four main components:

***Confidentiality*** - Protecting sensitive information from unauthorised disclosure or intelligible interception;

***Integrity*** - Safeguarding the accuracy and completeness of information and computer software;

***Availability*** - Ensuring that information and services are available when required;

***Privacy*** – University information will be compliant with current legislation

This Information Security Policy defines the principles for establishing effective security measures to ensure the confidentiality of University information that is held on computer systems. It also covers the continued availability of information and computer systems to support critical activities, and the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification, erasure or copying.

University information remains the property of the University irrespective of its storage medium

The University will take appropriate due care of information held on behalf of other parties. Examples can include joint research and shared jobs or functions.

## ***2. Security principles for UNSW***

### ***2.1 Protection of information***

***The systems and technologies used across the various UNSW faculties will protect the integrity, confidentiality and availability of sensitive information.***

#### ***Rationale***

University information is relied on by UNSW to provide services to students and perform its role as a university.

The reputation of the University would be adversely affected if the integrity of information, the protection of sensitive information, or the ability to continue processing after a disaster were compromised or identified as inadequate.

#### ***Implications***

The University will implement business controls to manage integrity and protect confidentiality of sensitive University information. The University will assess the risks and implement cost effective security controls to protect its environment.

Appropriate business continuity and disaster recovery plans will be developed, tested and implemented.

### ***2.2 Systems Access Controls***

***Only the internal major administrative systems and networks within the UNSW environment will be considered trusted. Security controls must be in place to ensure protection against un-trusted systems.***

#### ***Rationale***

The University needs to identify means of providing sensitive information and services to authorised users, but protect that information from access or disclosure to outsiders. Certain agreed information advertising University services is required through public views (eg web pages) to anyone.

#### ***Implications***

The University will implement appropriate controls to display public information while sensitive information will only be available to authorised University users. Security controls will be implemented to maintain protection levels over sensitive UNSW information. Other non-critical information may be made available to wider University user populations.

### **2.3 Access Privileges – (Minimum possible privilege)**

***Access to sensitive UNSW information and systems will only be granted on a need-to-know basis. All authorised users will be held accountable for their actions. Minimum possible privilege will be applied to all requests for access to sensitive systems.***

#### ***Rationale***

The nature of the role of the University gives insight to the huge variety of information generated by and used throughout the University. The security controls need to identify who needs what level of access to which information. Only the minimum levels of access required to enable users to perform their role, will be provided.

#### ***Implications***

The University will ensure that the different types of users are provided access tailored to their needs, and to the specific information required to satisfy those needs. These controls will ensure that the University complies with legislative requirements, and satisfies best practice in regard to protecting sensitive information.

### **2.4 Remote access**

***The systems and technology tools used across the University (including in the faculties and units) allow secure access to sensitive information for off-campus authorised users.***

#### ***Rationale***

Access to sensitive University information through remote access services requires the same level of confidence that the controlled information is only made available to authorised users as for on-campus users. Once authorised users have satisfied the security requirements for remote access, they should receive the same levels of security access as they would by being onsite. Remote access includes the risk that a user attempting to gain access may not be a genuine user.

#### ***Implications***

Controls will ensure that only authorised users are allowed to access sensitive University information remotely, and that the security access they receive is controlled according to the same principles as similarly-authorized onsite users.

### **2.5 Business Risk based controls**

***UNSW will implement security controls to manage risk to the University.***

#### ***Rationale***

Security controls can be costly to establish and implement. The University needs to ensure that before controls are implemented, it has considered the value of the information covered by these controls, and understood the likely threats against that information.

### ***Implications***

Controls will be appropriate for protecting elements of sensitive and confidential University information in compliance with current legislation. Information Owners and Systems Owners will be responsible for the assessment and implementation of risk management controls over the University information and systems, for which they have ownership responsibility.

## **2.6 Classification of UNSW information**

***Information from the various faculties, schools and units across UNSW will be consistently and appropriately classified and protected at all times.***

### ***Rationale***

While the University makes public much of its information through for example class materials, there is a need to ensure all information is consistently identified, valued, protected, suitably stored and managed to satisfy legal requirements, and protect the intellectual property owned by the University.

### ***Implications***

All information will be classified consistently. This minimises the risk that some sensitive information is not protected adequately, or that other information may be over-protected.

All authors and information owners will become familiar with the University standards and guidelines on classifying information and providing appropriate protection.

## **2.7 UNSW Information ownership**

***Intellectual property belonging to UNSW remains the property of UNSW. If it is taken off-site, the guidelines must be followed to protect UNSW property. All sensitive information and systems across UNSW faculties, schools and units must have owners.***

### ***Rationale***

University information is the most valuable intangible asset of UNSW. The University retains ownership of its intellectual property, whether that information is stored on UNSW IT systems, class teaching resources, student laptops, CDs or diskettes, both on University grounds and when taken off-site.

Refer to Section 12: Related Documents, item 7 regarding the University's Intellectual Property Policy

A number of Senior Officers of UNSW have been identified as owners of their faculty or unit's IT business information and related IT Systems. Information owners and Systems Owners must ensure that sensitive UNSW information and systems are

correctly managed at all times to protect UNSW intellectual property, and enable compliance with relevant laws and regulations.

### ***Implications***

Security measures will be implemented commensurate with the value to the University, to protect critical and sensitive information and systems.

Information owners will be responsible for managing their UNSW information, classification, protection appropriate for the information, and approving access to authorised users.

Systems owners will be responsible for managing the UNSW IT Systems and associated information; classification; protection appropriate for the system and; approving access to authorised users.

## **2.8 Security exceptions will be managed**

***IT security exception issues will be managed according to the UNSW Security Policy on a case by case basis.***

### ***Rationale***

UNSW will monitor the IT Security environment to ensure that exceptions, violations and other attempts to gain access without authorisation are identified, and managed consistently to protect UNSW information and IT systems.

### ***Implications***

Accidental and deliberate situations will arise where UNSW information may be at risk. The University will implement processes and procedures to monitor and manage security exceptions.

## **2.9 Enforceable and Practical Policies**

***The UNSW Security Policies will be enforceable and implementable.***

### ***Rationale***

The University supports large numbers of students from varying backgrounds, and must be sure they are all provided with an equal opportunity to undertake their education. The processes by which the education is delivered and the services provided must be fair for all; protect University resources and; establish a reliable environment for study.

### ***Implications***

The University will ensure enforcement of the IT Security policy. The policy cannot provide a deterrent to those who disregard the directions unless each case is addressed appropriately.

## **2.10 Compliance with legal and regulatory obligations**

***The systems and technologies used within UNSW will comply with legal and regulatory obligations including the Privacy Act and the Freedom of Information requirements.***

### ***Rationale***

Privacy Legislation requires all Australian businesses to protect various types of confidential information. Further federal legislation requires protection of tax file numbers, and Freedom of Information that enables the subject of information held to confirm details.

Best business practice requires access be provided to fulfil the specific role only. If the role changes, the security access privileges must change as well. Failure to satisfy legislative requirements can result in substantial fines and adverse publicity for the University.

### ***Implications***

The University will comply with all legislative requirements.

If there is a conflict between this security policy and legislative, the legislation requirements will prevail.

## **2.11 Standards acknowledged**

***Approved standards and processes will support security controls implemented to protect UNSW information, systems and services.***

### ***Rationale***

By adopting relevant standards, the University information systems are able to benefit from nationally or internationally agreed best practice for protecting and managing information, and IT systems used to process and maintain that information.

By following these standards the University has higher confidence that there is less likelihood for important aspects of security to be overlooked or incorrectly covered.

### ***Implications***

The University will develop and implement procedures that are supported by approved standards and processes.

## **2.12 Inform users of policy**

***No policy is enforceable unless users have read it. Policy must be brought to the users' attention.***

### ***Rationale***

With a large number of authorised users, the ability to provide awareness of security policies is a challenge.

Some users may claim they have not been informed of the policies or policy changes, or their security obligations identified in the policies.

If users are not informed, they may not understand their obligations to the security policies.

### ***Implications***

The University will ensure that a range of delivery channels will be used to make sure all users are informed about the IT Security policies, standards and guidelines.

All authorised students and staff will be made aware of the security controls, and their obligations in following the policy directions.

## ***3. Information Assets, Classification and Responsibility***

*This policy section links to security principles 2.5 – Business risk based controls, 2.6 – classification of UNSW information, and 2.7 – UNSW information ownership.*

### ***3.1 Information Assets and Inventory***

All major information assets will be accounted for and have a designated owner. An inventory will be drawn up for major assets associated with each IT system, each of those assets identified and ownership details and security classification documented. Any situations where joint ownership may occur will be negotiated with a mutually-acceptable arbitrator and the outcome communicated to the Chief Information Officer, DIS.

### ***3.2 Information Classification***

Owners of major information assets will classify the assets to designate an appropriate level of protection.

### ***3.3 Allocation of Information Security Responsibilities***

The owner of an asset may delegate their security responsibilities to others, but the owner of an asset will remain ultimately accountable for its protection. The delegate or custodian will share responsibility for information under their care.

### ***3.4 Risk Analysis***

Owners of information assets must conduct a risk analysis. When a risk analysis exercise has been performed, the appropriate procedures must be put in place to minimise exposure to that risk.

### ***3.5 Security of Third Party Access***

Access to University facilities by third parties will not be provided unless appropriate security measures have been implemented and a contract has been signed defining the terms for the connection. Third parties are generally identified as those business entities, or organisations, providing IT services to the University.

Affiliates are identified as other institutions, organisations or entities working in partnership with the University in delivering education and/or supporting research.

Both third parties and affiliates will be provided with appropriate access to specified University-managed IT Systems.

Users from these environments are subject to the same authentication and approval processes as authorised users and must comply with the same policies and procedures.

Contracts with IT related 3<sup>rd</sup> Parties must include Service Level Agreements that specifically cover how the 3<sup>rd</sup> party will manage UNSW information. UNSW retains a right to audit information management procedures of the 3<sup>rd</sup> party.

*(Refer to Section 12: Related Documents - items 4 and 5 regarding Privacy legislation)*

## ***4. System and Information Access Control***

*This policy section links with security principles 2.1 – protection of information, 2.2 – systems access controls, 2.3 – access privileges, and 2.4 – remote access.*

### ***Access policies and procedures***

Access to computer facilities managing and processing sensitive University information will be controlled by restricting access to authorised users only.

In the case of multi-user computer systems, the following is required:

1. Access to Administrative computer services and information will be controlled on the basis of need, that is access should only be granted for specific purposes, such as to fulfil the requirements of a course being delivered, or to perform a particular University function or role.
2. Identification and verification of the identity of each authorised user via an effective authentication process.
3. An appropriate automated means of recording potentially damaging access to sensitive systems from both local and remote locations
4. Provision of an access management system.

Access to non-critical systems may not require specific access for users.

## ***5. User Education and Responsibilities***

*This section links to security principles 2.3 – access privileges, 8 – security exceptions, 9 – enforceable and practical policies and 12 – inform users of policy.*

The University IT Security Policy will be made available to and brought to the notice of all authorised users.

The Policy provides information on users' responsibilities.

All users are responsible for keeping their personal authentication codes (e.g. passwords) secret and confidential (similar to a banking card PIN).

Users of UNSW IT facilities and services must not subvert UNSW security measures.

*(Refer also to Section 12: Related Documents item 1 – Rules relating to use of computing and electronic communication facilities)*

### ***5.1 User's Acceptance of Responsibilities***

For sensitive UNSW systems, users will be uniquely identified and will be personally accountable for all actions performed using their identification. Access must not be shared at any time. Disciplinary action may be taken against any user found to breach this policy.

Authorised users should be required to sign an undertaking that they have received, read and agree to abide by the IT Security Policy. This must be completed before access is provided.

*(Refer also to Section 12: Related Documents item 3 - UNSW Code of conduct)*

Staff users will be asked annually by the Vice Chancellor, to reconfirm their acceptance of the University IT policies, and their compliance to them.

### ***5.2 Authentication***

Users will keep their authentication (password) confidential.

Where approved workgroup accounts are operative, workgroup account authentication (passwords) will be kept solely within the workgroup. The authentication code will expire on completion of the workgroup task.

### ***5.3 Unattended Equipment***

Unattended equipment will have appropriate security protection implemented. This can include automatic locking, auto log out, or physical security controls.

Users remain responsible for breaches performed at unattended or unlocked equipment.

### ***5.4 Breaches of Policy***

Information Owners must establish procedures to manage security breaches. Breaches will be managed in accordance with the level of risk generated, and may include reporting to the Registrar and / or to HR as appropriate.

These procedures should include reporting instructions to be followed by staff and students if they observe a security breach.

University students or staff found to have breached the policy may face appropriate disciplinary action.

Third party Users who have breached the security policy will be escorted from University premises (if on campus) and may have their contracts cancelled.

*(Refer also to Section 12: Related Documents item 2 – Policy for making complaint or reporting incident....)*

## ***6. Physical and Environmental Security for Critical and Sensitive Information***

*This section links with security principles 2.1 – protection of information, and 2.7 – UNSW information ownership.*

### ***6.1 Facility Security***

IT facilities supporting critical or sensitive activities will be housed in secure areas with appropriate entry controls and security barriers, and physical protection from damage and interference.

### ***6.2 Clear Desk Policy***

Organisations should adopt a "Clear Desk Policy" for confidential and sensitive UNSW papers, storage media and other assets, in order to minimise the risks of unauthorised access, theft or damage outside normal working hours.

### ***6.3 Removal of Property***

Sensitive and confidential University information on any form of electronic media must not be taken off-site without appropriate permission from the Information Owner, or Systems Owner.

### ***6.4 Equipment Security***

Equipment will be physically protected from security threats and environmental hazards.

## ***7. Computer and Network Management***

*This section of the policy links with security principles 2.1 – protection of information, 2.5 – Business Risk based controls, and 2.8 – security exceptions.*

University systems will be maintained by appropriately trained staff.

### ***7.1 Operational Procedures and Responsibilities***

Responsibilities and procedures for the management and secure operation of all computers and networks will be established.

#### ***7.1.1 Documented operating procedures***

Documentation will be available to all users of computer systems to ensure their correct, secure operation.

#### ***7.1.2 Incident management procedures***

Incident management procedures and responsibilities will be established to ensure a quick, effective, and orderly response to security incidents.

### ***7.2 Protection from Malicious Software and Viruses***

All computers and computer systems should be protected to prevent / detect the introduction of malicious software and viruses.

### ***7.3 Network security controls***

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access.

Network infrastructure will be protected from unauthorised access.

### ***7.4 Electronic mail***

Electronic communication is not a secure medium. UNSW Organisations and faculties are required to adhere to the requirements of the UNSW Email Policy

*(Refer also to Section 12: Related Documents item 6 – UNSW Email policy)*

### ***7.5 Internet Use***

UNSW IT resources must be used responsibly when accessing research or other information through the Internet. The University will develop a set of “UNSW Acceptable Internet Usage” guidelines.

## ***8. Security Requirements of IT Systems***

*This section of the policy links with principles 2.1 – protection, and 2.7 – UNSW Information ownership.*

### ***8.1 Business risk analysis***

An analysis of the security requirements will form part of any proposal to acquire or maintain UNSW information systems, to ensure the resulting system complies with the IT Security Policy.

### ***8.2 Regular security review***

The IT Security policy requires regular review of the security measures implemented in UNSW information systems to maintain compliance with the Policy.

## ***9. Business Continuity Planning***

*This section of the policy links with security principle 2.1 – protection of information, (particularly the availability aspect)*

Business Continuity plans will be developed, implemented, and regularly tested to protect critical assets, systems and processes from the effects of major failures or disasters.

Information owners will determine the criticality of every UNSW IT System and develop appropriate auditable measures to ensure the required availability.

## ***10. Compliance with Legal Requirements***

*This section of the policy links with security principles 2.10 – compliance with legal and regulatory obligations, and 2.11 – standards acknowledged.*

All relevant contractual and statutory requirements will be explicitly defined and documented for each IT system, and the specific controls and responsibilities to meet these requirements will be defined and documented.

### ***10.1 Compliance with IT Security Policy***

All areas of the University will be considered for regular review to ensure compliance with the IT Security Policy.

### ***10.2 Compliance with legislation***

If there is a conflict situation between this policy and legislation, the legislation will prevail to the extent of the conflict.

*(Refer also to Section 12: Related Documents - items 4 & 5 on privacy)*

## 11. Definition of Terms

- Affiliate** - A research institution, training hospital or other entity working in partnership with the University in delivering education to students and / or supporting research for aspects of their education. May include government departments supporting the University.
- Asset** - Something of value.
- Authentication** - The confirmation of the identity of a user by providing a secret component (password or token details) that in combination with the user account details helps ensure only authorised users are gaining access to UNSW systems and information.
- Authorised Users** – the university students who are undertaking UNSW courses, the University staff and others specifically authorised to use UNSW facilities to perform their roles for the University.
- Availability** - Ensuring that information and vital services are available to users when required. Generally requires business continuity planning and various levels of recovery capability for both manual and IT based processes.
- Clear Desk policy** – Users must leave their work areas clear of all sensitive UNSW information at the end of their working day. Laptop computers must be either taken with the owner, or locked in a suitable lockable cabinet. Electronic media (eg CDs, diskettes, removable hard disks) must be locked in suitable security storage when not in use. Paper documents are to be appropriately filed and locked away.
- Confidentiality** - Protecting sensitive information from unauthorised disclosure or intelligible interception.
- Data** - the representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation, or processing by human or by automatic means.
- Freedom of Information** – The legal requirements and obligations for the University to provide details held on an individual – to the subject of that information.
- Information** - the meaning that is currently assigned to data by means of the conventions applied to those data.

**Information owners** – UNSW staff or students who create intellectual property at UNSW, for example academic papers, thesis notes, research information, and who are responsible for classifying that information, identifying risks, and in establishing appropriate protection for the information.

**Information technology** - the scientific, technological and engineering discipline and the management of techniques used in data handling and processing; their applications; computers and their interactions with people and machines; and associated social, economic and cultural matters.

**Integrity** - the accuracy and completeness of information and computer software.

**Major Administrative System(s):** The University's major administrative systems – eg Finance, HR and Student

**Major Information Asset** – Information classified as critical to the University and held on any form of electronic media

**Organisation** - group of people collectively responsible for a defined set of activities e.g. a Faculty, a School, an administrative unit, a research centre.

**Privacy** - the protection of personal information in compliance with privacy principles and current federal and state legislation.

**Risk analysis** - comprehensive concept for defining and analysing threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security measures.

**Security incident** - any event that has, or could have, resulted in loss or damage to organisational assets, or an action that is in breach of organisational security procedures.

**Sensitive information** – Information that could be included under privacy, freedom of information, copyright, intellectual property or patent legislation or policies

**Sensitive system** – A system that stores, processes and maintains sensitive information.

**Service Provider** - an individual or group providing access to information, IT or IT systems.

**Systems Owner** - an individual or faculty having responsibility for specified information system assets and for the maintenance of appropriate security measures.  
The responsibility of the processing of the information and running of the system can be delegated to a custodian, who will maintain the required security measures.

**User** - individual or organisation authorised to make use of information or information technology.

**User ID** - Login name or token used to identify a user of an IT system. Usually used with a secret means of authentication (password) known only to the user.

## ***12. Related Documents referenced in the policy***

1. ***Rules Relating to the Use of Computing and Electronic Communication Facilities at the University of New South Wales,***

<http://www.infonet.unsw.edu.au/poldoc/rulcomp.htm>

2. ***Policy for making a complaint or reporting incidents of criminal, corrupt conduct or maladministration or Protected Disclosure at UNSW,***

[http://www.infonet.unsw.edu.au/poldoc/protected\\_disclosure.htm](http://www.infonet.unsw.edu.au/poldoc/protected_disclosure.htm)

3. ***UNSW Code of Conduct,***

<http://www.hr.unsw.edu.au/poldoc/codecond.htm>

4. ***Privacy and Personal Information Protection Act 1998 (NSW),***

[http://www.austlii.edu.au/au/legis/nsw/consol\\_act/papipa1998464/index.html](http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/index.html)

5. ***Privacy Act 1988 (Commonwealth),***

<http://scaleplus.law.gov.au/html/pasteact/0/157/top.htm>

6. ***UNSW Email policy,***

<http://www.infonet.unsw.edu.au/poldoc/email.htm>

7. ***UNSW Intellectual Property Policy,***

<http://www.infonet.unsw.edu.au/poldoc/ippol.htm>

8. ***UNSW Privacy Management Plan,***

<http://www.privacy.unsw.edu.au/pmp.htm>

9. ***Student Misconduct Rules,***

<http://www.infonet.unsw.edu.au/poldoc/stumis.htm>