



THE UNIVERSITY OF
NEW SOUTH WALES

***UNSW IT Security
Standards & Guidelines***

UNSW IT Security Standards

DIVISION OF INFORMATION
SERVICES

Effective from
March 2004

Table of Contents

<i>Preamble</i>	3
1. INTRODUCTION	3
1.1 <i>Environment</i>	3
1.2 <i>Threats</i>	3
1.3 <i>Scope and Application of Information Technology Security</i>	4
2. SECURITY PRINCIPLES FOR UNSW	4
3. INFORMATION ASSETS, CLASSIFICATION AND RESPONSIBILITY	5
3.1 <i>Information Assets and Inventory</i>	5
3.2 <i>Information Classification</i>	5
3.3 <i>Allocation of Information Security Responsibilities</i>	5
3.4 <i>Risk Analysis</i>	5
3.5 <i>Security of Third Party Access</i>	5
4. SYSTEMS AND INFORMATION ACCESS CONTROL	6
4.1 <i>Access policies and procedures</i>	6
4.2 <i>Secure Authentication Process</i>	6
4.3 <i>Access Management System</i>	7
4.4 <i>Information systems Access Control</i>	7
4.5 <i>Monitoring System Access and Use</i>	7
5. USER EDUCATION AND RESPONSIBILITIES	8
5.1 <i>User's Acceptance of Responsibilities</i>	8
5.2 <i>Authentication</i>	8
5.3 <i>Unattended Equipment</i>	9
5.4 <i>Reporting of Breaches of Policy</i>	9
6. PHYSICAL AND ENVIRONMENTAL SECURITY FOR CRITICAL AND SENSITIVE INFORMATION	9
6.1 <i>Facility Security</i>	9
6.2 <i>Clear Desk Policy</i>	10
6.3 <i>Removal of Property</i>	10
6.4 <i>Equipment Security guidelines</i>	10
7. COMPUTER AND NETWORK MANAGEMENT	11
7.1 <i>Operational Procedures and Responsibilities</i>	11
7.2 <i>Incident management procedures</i>	11
7.3 <i>Protection from Malicious Software</i>	11
7.4 <i>Virus controls</i>	12
7.5 <i>Network Security Controls</i>	12
8.0 SECURITY REQUIREMENTS OF IT SYSTEMS	13
9.0 BUSINESS CONTINUITY PLANNING	13
10. COMPLIANCE WITH LEGAL REQUIREMENTS	14
11. DEFINITION OF TERMS	15
APPENDIX A	17
EFFECTIVE PASSWORD MAINTENANCE	17
CHOOSING A GOOD AUTHENTICATION CODE / PASSWORD	17
SAMPLE AUTHENTICATION CODES / PASSWORDS	17

Preamble

(Information)

University of NSW IT Security information is contained in a series of documents. The UNSW IT Security Policy, these IT Security Standards and Guidelines, and other guideline documents referred to at the end of the Policy document. In the IT Security Policy there are three discrete levels of issues related to IT Security. These include the security principles, the policy statements, and in this document, the IT Security standards and guidelines. The policy statements are the intentions of University management and are based on the security principles.

The IT security standards provide how-to instructions and guidelines for users. A series of definitions is included at the end of the IT Security Policy, and this document.

1. INTRODUCTION

(Standard)

The University maintains agreements and co-operative arrangements with others, such as other universities, hospitals, companies and government departments and bodies, and any of these relationships may have an information component and include information security requirements. The University must also respect and abide by State and Federal law, including those pertaining to copyright and Privacy. 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.

Universities have historically been seen as a place of openness, where information is freely communicated to the betterment of students wishing to further their education and to aid in the increase and dissemination of knowledge. The University's IT Security Policy recognises the scale and complexity of the environment, as well as the ethos of the institution.

1.1 Environment

The University Information Technology (IT) environment is extremely diverse and complex, and includes:

- central computer systems containing financial, human resources, students' records, assets, planning, corporate and personal information.
- computer systems maintained by Faculties, Schools and other units which may contain copies of central information either in their original form or modified in some way, local administrative information, academic (research/teaching) information, or the personal information of staff and students.
- smaller computer systems ranging down to desktop units that may contain some information similar to that above, but usually contain research or teaching data or systems, or personal information.
- computer networks that link all of the systems above within the University community, as well as linking them to national and international networks.

Much of this information must be maintained confidentially or be used in ways prescribed by law. Other information would be very costly to replace, or would lead to other negative impacts if lost or compromised.

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

The University maintains agreements and co-operative arrangements with others, such as other universities, hospitals, companies and government departments and bodies, and any of these relationships may have an information component and information security requirements. The University must also respect and abide by State and Federal law, including those pertaining to copyright and Privacy.

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

Universities have historically been seen as a place of openness, a place where information is freely communicated to the betterment of students wishing to further their education and to aid in the increase and dissemination of knowledge.

The University's Information Security Policy recognises the scale and complexity of the environment, as well as the ethos of the institution.

1.2 Threats

IT systems and networks may face a variety of threats including computer-based fraud, espionage, vandalism, accident, natural disaster, computer viruses and computer hackers, and as the world's dependence on IT continues to increase, so the threats become more widespread, more ambitious and increasingly sophisticated. Failure to maintain confidentiality, integrity or availability of information and IT systems will have financial and other outcomes that are often underestimated. As with many other things in life, prevention is better than cure. By taking action now to safeguard information and IT systems, the University reduces its exposure to threat, and reduces the likelihood of negative outcomes in the future.

1.3 Scope and Application of Information Technology Security

The Information Technology (IT) Security Policy is to be implemented in all areas of the University as a basic policy. However, the policy and these standards cover a very wide range of issues, and not all areas of the policy and standards will be directly applicable in all areas of the University. For example, the policy on passwords may not be relevant on IT systems that do not require a password. The section on documenting operational procedures will be more relevant, and produce more detailed documentation for a large multi-user system than for an isolated personal computer on a desk.

These standards may be extended by organisations within the University based on risk assessment, statutory or contractual requirements or unique principles, objectives or requirements. For example, the central IT resource providers within the Division of Information Services will have statutory, contractual or managerial requirements which will be combined with the policy and standards to create a more strict set of controls for use in these areas.

2. SECURITY PRINCIPLES FOR UNSW

(Information)

The UNSW IT Security policy includes a series of security principles on which security for the University is based. The principles include the following areas;

- 2.1 Protection of information
- 2.2 Systems access controls
- 2.3 Access privileges
- 2.4 Remote access
- 2.5 Business risk based controls
- 2.6 Classification of UNSW information
- 2.7 UNSW Information ownership
- 2.8 Security exceptions will be managed
- 2.9 Enforceable and practical policies
- 2.10 Compliance with legal and regulatory obligations
- 2.11 Standards acknowledged
- 2.12 Inform users of policy

These principles help the University determine criticality of systems, levels of protection required, and ensure that appropriate controls are implemented to protect University intellectual property and satisfy legal requirements.

These standards and guidelines provide more details for implementation of policy directions.

3. INFORMATION ASSETS, CLASSIFICATION AND RESPONSIBILITY

3.1 Information Assets and Inventory

(Standard)

All major information assets will be accounted for and have a designated owner. An inventory will be drawn up for major information 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

(Guideline)

A matrix to assist in the classification of information is being developed and will be appended to this document at a later date..

Other information owners or authors creating original material to be stored electronically may also wish to consider identifying and classifying these assets in order to designate an appropriate level of protection of the information.

These information assets may or may not involve intellectual property and could range in nature from original research material to a local FilemakerPro database set up to assist administrative tasks.

3.3 Allocation of Information Security Responsibilities

(Standard)

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

3.4 Risk Analysis

(Standard)

Where a risk analysis has been performed, the appropriate procedures must be put in place to minimise exposure to that risk.

3.5 Security of Third Party Access

(Standard)

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 that provide IT services to the University.

Other relationships with Government departments, teaching hospitals and research institutes are recognised, for the purposes of these standards, as affiliates of the University, and are provided with access to specified University-managed IT Systems. These environments provide extended education to UNSW students and practical training in their specific subject fields.

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

To provide for situations where 3rd party users are found to be in breach of the IT Security Policy, their contracts should include standards clauses allowing the UNSW to cancel that contract without penalty. This would only be exercised in serious breaches of policy.

4. SYSTEMS AND INFORMATION ACCESS CONTROL

4.1 Access policies and procedures

(Standard)

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

Each Service Provider within the University community should maintain a defined user access policy statement which should take account of :-

- The security requirements of individual unit's information systems
- Policies and standards for information dissemination and entitlement (e.g. need to know principle)
- Security profiles may be established for common access categories.
- The use of Special Privileges should be restricted and controlled as unnecessary allocation and use of system privilege is a major contributing factor in the vulnerability of systems.
- There should be formal user registration and deregistration procedures.

Access to multi-user IT services should be controlled through a formal registration process which should :-

- check that the user has authorisation from the system owner for use of the service;
- check that the level of access is appropriate;
- give users a written statement of their access rights and responsibilities;
- require users to sign undertakings to indicate that they have read the IT Security policy and understand the conditions, level and type of access they have been granted;
- ensure access is not granted until the registration procedures have been completed;
- maintain a formal record of all persons registered to use the service, and the expiry time/method etc to remove access;
- ensure that access is removed promptly at the end of the registered period;
- periodically check for and remove expired/redundant accounts;
- ensure that redundant user IDs are not reissued to another user.

Wherever possible, do not create "guest" or anonymous accounts, and if these accounts are required they should be given minimal access rights and their use should be strictly monitored.

In the case of multi-user computer systems processing UNSW administrative information, the following is required:

- Identification and verification of the identity of each authorised user via an effective authentication process.
- ***Providing an appropriate automated means of recording potentially damaging access to sensitive systems from both local and remote locations.***
- Providing an access management system that ensures quality authentication codes.
- Where appropriate, restricting the connection times of users and implementation of time-out thresholds.

Note that access to non-critical systems may not require specific access for all users.

4.2 Secure Authentication Process

(Guideline)

The following checklist should form an integral part of any secure logon process.

- Display a general notice warning that the computer must only be accessed by authorised users.
- Limit the number of unsuccessful logon attempts allowed before action is taken (3-4 attempts are recommended) to:

- Record the unsuccessful attempt.
- Force a time delay before further logon attempts are allowed.
- Disconnect data link connections.
- Display the following information on completion of a successful logon:
 - Date and time of the previous successful logon.
 - Details of any unsuccessful logon attempts since the last successful logon.

4.3 Access Management System

(Guideline)

An effective access management system should be used to authenticate users, and provide controls to set minimum authentication code standards, thereby ensuring that users have quality authentication codes (passwords).

A good access management system should:

- Enforce the use of individual authentication codes to maintain accountability.
- Allow users to select and change their own authentication code and include a confirmation procedure to allow for typing errors.
- Enforce a minimum length for authentication codes (a minimum of 6 or 7 characters is recommended).
- Enforce a change of authentication code at regular intervals.
- Force users to change temporary authentication codes at the first logon.
- Maintain a record of previous user authentication codes and prevent them from using the most recent ones for a specified period of time (6 months is recommended).
- Never display the authentication code on screen while it is being entered.
- Store authentication codes in encrypted form using a one-way encryption algorithm.
- Alter default vendor authentication codes following installation of software.
- If possible, check that the authentication code is not based on any of the following:
 - Months of the year, days of the week or any other aspect of the date.
 - User ID, user name, group ID or other system identifier.
 - More than 2 consecutive identical characters.
 - All-numeric or all-alphabetic groups.

4.4 Information systems Access Control

(Standard)

Information systems (those that capture, store and process sensitive information) should have logical access controls to manage access in the following ways:

- Control user access and system functions in accordance with a defined access control policy.
- Provide protection from unauthorised access for any utility software that is capable of overriding operating system or information system controls.
- The access controls should not compromise the security of other systems with which IT resources are shared

4.5 Monitoring System Access and Use

(Standard)

Information Systems should be monitored to ensure conformity to access policy and standards. In order to have effective monitoring and audit tools, it is essential that logging of potentially damaging events – including exceptions, violations and other security-relevant events be performed, monitored and kept for a recommended period of time.

Where possible, event logs should include User Ids, dates and times, and node address or terminal identifier.

All system clocks should be adjusted to the correct time on a regular basis (at least monthly) to simplify event tracking between multiple systems.

5. USER EDUCATION AND RESPONSIBILITIES

(Standard)

The University IT Security Policy will be made available to and brought to the notice of all authorised Users. In addition to appropriate training in the correct use of IT facilities and software packages, all users should be made aware of information security threats and concerns, and should be equipped to support the University's IT Security Policy in the course of their normal work. Users of UNSW IT facilities and services must not subvert UNSW security measures.

5.1 User's Acceptance of Responsibilities

(Standard)

Users should be required to sign an undertaking that they have received, read and agree to abide by the IT Security Policy. Users should always keep in mind that the information and IT resources to which they have been granted access are to be used only for authorised University purposes. Users should be aware that they are responsible for actions performed under their user ID/password combination, and that they may be held liable to the fullest extent of the law if they are negligent in their responsibilities associated herewith. For sensitive UNSW systems, Users are to be uniquely identified and 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.

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

Regulations and laws that may be relevant include the University Rules on Student Misconduct, the Crimes Acts of various States and Territories, and the Federal Privacy, Freedom of Information and Crimes Acts.

5.2 Authentication

(Standard)

Users will keep their authentication codes (passwords) confidential.

Where workgroup accounts are used in research projects and similar exercises, workgroup account authentication codes will be kept solely within those workgroups. It is recommended that the authentication code should expire when the workgroup tasks have been completed. Workgroup accounts are discouraged as they do present problems with determining accountability for actions performed by various workgroup members.

When a user account is first created the user should be provided with a secure temporary authentication code (password), which they are forced to change immediately. If a user forgets their authentication code, they should again be provided with a secure temporary authentication code, which they are forced to change immediately. All users should be required to provide photo identification to have their authentication code re-set.

Users should refer to Appendix A for advice on good practices regarding authentication code maintenance and choice.

Access rights of users should be reviewed regularly with a maximum period of 6 months between reviews. Access rights for privileged accounts should be reviewed more frequently.

5.3 Unattended Equipment

(Guideline)

Unattended equipment will have appropriate security protection implemented.

This can include the controls to help with automatic locking, auto log-out or time-out, and physical security controls such as door locks on storage cabinets and activity rooms.

Users remain responsible for breaches performed at unattended or unlocked equipment

Following are some good practices that all users should adopt;

- Terminate active sessions when finished, unless they can be secured by an appropriate logical lock on the screen.
- Log off correctly from all computers. Don't just switch off the machine.
- Secure the computer so that an authentication code is required to re-activate, or physical key lock. Lock the room where the computer resides if appropriate.

5.4 Reporting of Breaches of Policy

(Guideline)

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.

In cases where University students or staff have been discovered to have breached the policy, these cases may face appropriate disciplinary action.

It is recommended that 3rd party contracts include clauses so that Third party Users who have breached the security policy may be escorted from University premises (if on campus) and may have their contracts cancelled, without penalty to the University.

Incidents should generally also be reported to the user's supervisor or lecturer.

A user who is able, through use of an IT service, to gain access that they have not been granted during the registration process, must consider this a breach of security and report it immediately.

Any observed or suspected security weaknesses in, or threats to, systems or services should be reported. Users should not try to prove such a weakness. Users should also report software that does not perform according to specification, either to their local IT support unit or to the software or service provider.

In all cases above, the user should:

- Make written note of any commands, any symptoms and any messages appearing on the screen.
- Stop using the computer and isolate it physically if possible. It should be disconnected from any networks (with the assistance of a computing support officer) and left powered on, unless the user is concerned that files may be altered or erased if the computer is left powered on.
- Report the matter immediately to the user's supervisor or lecturer, who may in turn report the breach to the Registrar or HR if warranted.

6. PHYSICAL AND ENVIRONMENTAL SECURITY FOR CRITICAL AND SENSITIVE INFORMATION

The requirements for physical security will vary depending on the scale and organisation of IT services and the sensitivity or importance of the information and activities supported. However the appropriate implementation of equipment security measures outlined below should be considered.

6.1 Facility Security

(Standard)

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

Security barriers should reflect the value of assets and associated risks eg. a locked room; a purpose-built computer room; a PC anchor. Entry controls can include auditable access logs.

Personnel supplying or maintaining support services should only be granted access when required and authorised, and where appropriate, their access should be restricted and their activities monitored.

The selection and design of sites to house critical activities should take account of the possibility of fire, flooding and other natural and man-made disasters. Reserve equipment and backup-media should be stored off-site.

6.2 Clear Desk Policy

(Guideline)

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

Where appropriate the following should be considered:

- Sensitive and confidential papers, media and other assets should be locked in cabinets when not in use.
- Sensitive information, laptops, personal digital assistants (PDAs), and other valuable items should be locked away when not in use.
- Personal computers and computer terminals should be protected by key locks, authentication codes and other controls when not in use.
- Licenced software CDs and installation manuals should be stored securely to help protect the University's licencing rights.

6.3 Removal of Property

(Standard)

Sensitive and confidential University information on any form of electronic media must not be taken off-site without appropriate authorisation from the information owner or systems owner. Acknowledgment should be given to those authorised users with remote access, who perform University work from home.

6.4 Equipment Security guidelines

(Guideline)

Equipment will be physically protected from security threats and environmental hazards. Protection of IT equipment (including that used off-site) is necessary to both reduce the risk of unauthorised access to data, and to safeguard against loss or damage. The following checklist may be used to identify potential hazards;

- Fire
- Smoke.
- Water and other liquids.
- Dust.
- Vibration.
- Chemical effects.
- Electrical supply interference.
- Electromagnetic radiation.
- Theft.

Smoking, eating and drinking should be prohibited in computer areas.

7. COMPUTER AND NETWORK MANAGEMENT

University systems will be maintained by appropriately trained staff.

It is unreasonable to expect staff to correctly install and operate IT systems, or to comply with the IT Security Policy, if they lack the expertise or understanding to do so.

7.1 Operational Procedures and Responsibilities (Standard)

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

This includes the provision of an incident response procedure.

7.2 Incident management procedures (Standard)

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

Such a procedure would vary in scope depending on the sensitivity and size of the information systems being managed. A campus-wide Incident Management procedure will be established for all systems, and will be based on the evaluation of the risk from:

- system failures and loss of service;
- errors resulting from incomplete or inaccurate data; and
- breaches of confidentiality.

In the meantime, all incidents must be reported to the Help Desk (02) 9385 1333

Action to correct and recover from security breaches and system failures should be carefully and formally controlled. The procedures should ensure that:

- only authorised staff are allowed access to live information systems and data;
- all emergency actions taken are documented in detail;
- emergency action is reported to the responsible person or body and reviewed in an orderly manner; and
- the integrity of the information system and security controls are confirmed with minimal delay.

Managers of large or sensitive information systems should also consider including procedures, which cover:

- analysis and identification of incident causes;
- planning and implementation of remedies to prevent recurrence;
- collection of audit trails and similar evidence; and
- communication with users and others affected by or involved with the incident, including by means other than electronic in case of serious failure

Audit trails and similar evidence should be collected and secured, as appropriate for:

internal problem analysis;

use as evidence in relation to potential breaches of contract or breach of regulatory requirement;

negotiating for compensation from software and service suppliers; and

evidence in the event of proceedings under computer misuse or data protection legislation.

7.3 Protection from Malicious Software (Standard)

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

Precautions are required to prevent and detect the introduction of malicious software. A range of malicious techniques has been developed to exploit the vulnerability of computer software to unauthorised or unknown modification. For example, computer viruses, network worms, trojan horses and logic bombs. Managers of computers and computer systems should be alert to the dangers

of malicious software, and should take steps to prevent or detect the introduction of malicious software.

In particular, it is essential that precautions are taken to prevent and detect the currently known forms of malicious software and computer viruses on personal computers (PCs). This will require planned and tested processes for distributing updates to resolve identified system vulnerabilities.

7.4 Virus controls

(Guideline)

Virus detection and prevention measures and appropriate user awareness procedures should be implemented. Users should be reminded that prevention is far better than cure. The basis of protection against viruses should be founded on good security awareness, appropriate system access controls, and the following specific guidelines:

The school or group should establish a formal policy requiring compliance with software licenses and prohibiting the use of unauthorised software.

Anti-virus software developed by a reputable supplier should be used as follows:

- Virus-specific detection software (which must be regularly updated and used as directed by the supplier) should be used to scan computers and media for known viruses, as a precautionary measure for suspect files and on a routine basis.
- Change detection software should be installed on computers, where appropriate, to detect any change in executable code.
- Virus "repair" software should be used with caution, and only in cases where virus characteristics are fully understood and the correct repair is certain. "Call the HELP Desk"
- Consider conducting regular reviews of the software and data content of systems supporting critical processes. The presence of any spurious files or unauthorised amendments should be formally investigated.
- Any diskettes or CDs of uncertain or unauthorised origin should be checked for viruses before use.
- Management procedures and responsibilities should be established for reporting and recovering from virus attacks.
- Appropriate plans are to be established covering all necessary data and software backup recovery arrangements.

These measures are especially important for network file servers supporting a large number of workstations.

7.5 Network security controls

(Standard)

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.

A range of security controls is required in computer networks to protect these environments. Individual users should be aware that connecting their computer to the network can allow unauthorised access to private data if appropriate controls are not established. Documentation should be available to the user detailing how to adequately secure their data should they wish to make it available on a network. Please call the "HELP Desk" for assistance.

Network managers should ensure that appropriate controls are established to ensure the security of data in networks, and the protection of connected services from unauthorised access. Special attention is required to protect sensitive information passing over public networks like the Internet.

Tools are readily available which allow network ports to be monitored, or the operation of the network to be disrupted. In order to minimise the risk of network interference, consideration should be given to:

- Protecting cabling in public areas with conduits or other protective mechanisms.
- In a structured wiring area, ensuring that network and telephone points that are not in use have been detached from the active network or telephony equipment.
- Telephony and networking risers and data cabinets are only able to be accessed by authorised personnel.
- Information which is being transferred over a less secure network (eg the Internet), is encrypted.

Highly accessible access points such as networked modems should have associated appropriate security mechanisms.

8.0 SECURITY REQUIREMENTS OF IT SYSTEMS

(Standard)

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 Security Policy.

The IT Security policy and these standards require regular review of the security measures implemented in UNSW information systems to maintain security compliance.

Security requirements for IT systems must be identified and agreed as part of the requirements phase, prior to development.

The security requirements and controls should reflect the value of the information involved to the University, and the potential damage which might result from a failure or absence of security. Areas which can be considered include :-

- Segregation of facilities or duties.
- Access controls for information systems files and functions.
- Validation of input data. Design and use of control totals.
- Creation and regular review of audit trails for important events and attempted unauthorised access.
- Procedures, documentation and training to allow the system to be used securely by non-specialist staff.
- Creation and storage of backup copies of data and system.
- Recovery from failures, especially for high availability applications.
- Use of data encryption to protect data from unauthorised access, either during transmission or storage.
- Use of digital signatures to provide message authentication.
- Use of formal change controls to ensure testing and authorisation of updates.
- Use of version controls for IT system software and documentation.
- Protection of test data, by ensuring any production data is "depersonalised" before use and removed after testing.
- Restriction on access to system audit tools, to prevent misuse or compromise.

9.0 BUSINESS CONTINUITY PLANNING

(Standard)

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

Information Owners and Information Systems owners will determine the criticality of sensitive UNSW information and every UNSW IT system to develop appropriate measures that ensure the required availability.

This should include identification and reduction of risk, and the creation and testing of processes to resume essential operations.

Continuity plans should focus primarily on keeping essential processes and services running, including staffing and non-computing requirements, not merely on the fallback arrangements for computing services. Each plan should specify clearly the conditions for its activation, the individuals responsible for each component of the plan and the custodian responsible for the plan as a whole.

The continuity planning process should cover :-

- Determination of the impact of failure.
- Design of and agreement on emergency arrangements.
- Documentation of procedures, processes and responsibilities.
- Preparation and maintenance of any redundant assets - eg. offsite storage of backups, stationary, documentation, and equipment.
- Training for staff involved.
- Testing schedule for all components. Review and update of plan to match changes in the environment or IT processing.
- Communication with affected users in the event of a serious failure, including alternatives to electronic communication eg telephone.

10. COMPLIANCE WITH LEGAL REQUIREMENTS

(Standard)

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.

Proprietary software products are usually supplied under a licence agreement that limits the use of the product to specific computers.

Users of the software should be aware of the limitations imposed by the licence agreement and comply with them.

A register of software should be maintained for all IT systems and regular audits of software use should be undertaken.

Users should not copy software from one computer to another without the software owners documented consent.

11. DEFINITION OF TERMS

(Information)

- 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 -** Currently enrolled students who are undertaking UNSW courses, 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 -** Persons who create or are responsible for information stored in electronic format who are responsible for classifying that information, identifying risks, and in establishing appropriate protection for the information. This includes UNSW staff or students who create intellectual property at UNSW (for example academic papers, thesis notes, research information), as well as owners of information stored on major administrative systems.
- 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 -** The University's major administrative systems – eg Finance, HR and Student
- Major information asset -** Information classified as critical by 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, Patent or other relevant 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, unit 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.

APPENDIX A

EFFECTIVE PASSWORD MAINTENANCE

(Guidelines)

Password information should be treated in the same manner as your PIN on your bank account. Under Federal and State law you may be held responsible if you are negligent and your account is used as a tool for compromising system security.

Following is a set of guidelines, which should be followed when maintaining your authentication codes and User-ID's.

Use only those resources, facilities and data in respect of which authority you have been given.

- If you change school/faculty/unit/department or are leaving the University, you should notify the IT focal point/nominee and ask that the account be disabled.
Authentication codes / Passwords should not be revealed to anyone.
- If you suspect that your authentication code has been breached, change it immediately and report it to your IT focal point/nominee.
- Always log off or lock the screen when you are not there.

CHOOSING A GOOD AUTHENTICATION CODE / PASSWORD

Ensure a minimum authentication code / password length of 6-7 characters.

- Embed numeric or non-alphabetic characters within the authentication code
- Change your authentication code regularly.
- Do not re-use old authentication codes.
- Do not use more than 2 consecutive characters, (this makes it easy for someone looking over your shoulder to detect your authentication code).

Do not use the following items as part of your authentication code:

- Your name, or the name of your spouse, children, dog, cat etc.
- Your date of birth, telephone number, vehicle registration number etc.
- Months of the year, days of the week or any other aspect of the date.
- Your USERID or staff employee number.
- Words from any dictionary without any addition or modification of characters.

SAMPLE AUTHENTICATION CODES / PASSWORDS

2good4u
ren & stimp
mazda323
4camels
2for\$50
cat8dog
tim5tam
2000 olympics
500miles
million\$smile
comp7uter
1twoone2

Please do not use any of these sample authentication codes as your own.