THE UNIVERSITY OF SYDNEY

Information Security Policy

Last updated: 09 March 2010

Policy Assigned to: Chief Information Officer, ICT

Table of Contents

1. Overview

The policy provides management direction and support for information security in accordance with operational requirements, relevant laws and regulations. The policy is directly aligned with the Information Security Industry standard AS/NZS ISO/IEC 27002:2006: Information technology - Security techniques - Code of practice for information security management. Relevant sections from this standard are directly referenced in this document.

2. Background

Information is an asset that, like other important operational assets, is essential to the University of Sydney operations and consequently needs to be suitably protected.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it must be adequately protected.

Information security is the protection of information (including systems) from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximize return on investments and operational opportunities.

Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and University objectives of the organisation as met.

For each of the risks identified following the risk assessment a risk treatment decision is made. Options for risk treatment include:

a) Applying appropriate controls to reduce the risks;
b) Knowingly and objectively accepting risks, providing they clearly satisfy the organisation’s policy and criteria for risk acceptance;
c) Avoiding risks by not allowing actions that would cause the risks to occur;
d) Transferring the associated risks to other parties, e.g. insurers or suppliers;
e) Or a combination of the above options to treat residual risk.

3. Coverage

This policy covers all academic and general staff (including casual staff), students and affiliates.

4. Definitions

Affiliate means a clinical title holder, an adjunct, conjoint or honorary appointee, a consultant or contractor to the University, an office holder in a University entity, a member of any University Committee and any other person appointed or engaged by the University to perform duties or functions on its behalf.

Asset means anything that has value to the University of Sydney.

Availability means continuity of operational processes and recoverability in the event of a disruption.

Confidentiality means ensuring that information is accessible only to those authorised to have access

Control means a mechanism for managing risk. (E.g. Policy)

Data means both raw and processed data, including electronic data files, regardless of their storage media as well as information derived from processed data, regardless of the storage or presentation media.

Information asset is defined as any representation of knowledge concerning objects such as facts, events, things, processes, ideas or opinions that has a particular meaning within a certain context.

Information processing facilities means any information processing system, service or infrastructure, including the physical location housing them.

Information Security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. It includes the preservation of confidentiality, integrity and availability of information.

Integrity means the context of completeness, accuracy and resistance to unauthorised modification or destruction

ISMS means Information security management system as defined by AS/NZS 7799.2:2003.

Removable media means tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.

Risk is the chance of an event occurring that could have a negative or positive impact on the University achieving its objectives.

Risk Assessment means the process which considers information assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible defensive measures and their costs and estimated probable savings from better protection.

Secure areas - is where access is limited to authorised personnel only.

Sensitive data includes information assets classified at Internal or X-In-Confidence as per the Information Classification Policy – refer to section 7.2.

5. Risk Assessment and treatment.

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational harm likely to result from security failures.
The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.
Risk assessment must be repeated as often as necessary to address any changes that might influence the risk assessment results, but at least every 12 months.
Risk assessment must be completed as part of any project, to make sure that whatever is being changed/implemented will not have a negative impact on exiting risks or creating new ones.
ICT Information security team will manage this process. The asset owners will ultimately decide on how to treat (mitigate, reduce, accept, transfer) the risk.

6. Organisation of Information Security

Objective: To manage information security within the organisation.

- A management framework must be established by ICT to initiate and control the implementation of information security within the organisation.

6.1.1 Management commitment to Information Security

- Management must actively support security within the through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

6.1.3 Allocation of information security responsibilities

- All information security responsibilities must be clearly defined.
- Allocation of information security responsibilities must be done in accordance with this policy.

6.1.4 Authorisation process for information processing facilities

- A management authorisation process for all information processing facilities must be defined and implemented.

6.1.8 Independent review of information security

- The approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) must be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

7. Asset Management

Objective: To achieve and maintain appropriate protection of al assets.

- The asset owner determines the classification of the asset. All assets classified as sensitive must be accounted for and have a nominated owner. The nominated asset owner is responsible for delegating/approving access.

7.1 Responsibility for assets.

7.1.1 Inventory of assets

- All assets classified as sensitive must be clearly identified and an inventory of all important assets drawn up and maintained.

7.1.3 Acceptable use of Assets

- Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented, and implemented. See Acceptable Use Policy.

7a Information Classification Policy

7.2 Information Classification Policy

Objective: To ensure that information receives an appropriate level of protection. Sensitive Information must be classified to indicate the need, priorities, and expected degree of protection when handling the information.

7.2.1 Classification guidelines:

Information must be classified in terms of its value, legal requirements, sensitivity, and criticality to the University.

Sensitive classification refers to Internal and X-In-Confidence levels. Access to this information must be via an authentication process.

Default classification is Public. This information is freely available to both internal and external parties without the requirement for any authentication. E.g. Information is available on the internet.

There are 3 levels of classification:

(1) **Public**: The information maybe freely disclosed externally.

(2) **Internal:** Access is limited to employees of the University of Sydney.

(3) **X-In-Confidence:** Information whose compromise could cause limited damage to the University of Sydney. e.g.

- Cause substantial distress to individuals or private entities;
- Cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or private entities;
- Prejudice an investigation;
- Prejudice the integrity of any examination or other form of assessment, results or student records;
- Prejudice the conduct of research;
- Facilitate the commission of crime;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Impede the effective development or operation of the University of Sydney policies;

- Breach statutory restrictions on disclosure of information; Disadvantage the University of Sydney in commercial or policy negotiations with others;
- Undermine the proper management of the University of Sydney and its operations.

8. Human Resources Security

8.2 During employment or engagement

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

- Management responsibilities must be defined to ensure that security is applied throughout an individual's employment within the University.
- An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities must be provided to all employees, contractors and third party users to minimise possible security risks.
- Policies must be in place to facilitate the investigation of alleged breaches
- Appropriate disciplinary action must be taken in respect of security breaches.

8.3 Termination or change of employment or engagement

Objective: To ensure that employees, contractors and third party users exit the University or change employment in an orderly manner.

- Procedures must be in place to ensure that when the employment or engagement of an employee or Affiliate ends, their exit from is managed, and that the return of all equipment and the removal of all access rights are completed.
- Exit procedures should also be followed as far as appropriate where a staff member or affiliate is transferring to a new role or work location.

9. Physical and environmental Security – ICT Data Centre

Objective: To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

9.1.1 Physical security perimeter

- Information processing facilities managed by the organisation must be physically separated from those managed by third parties.
- Critical or sensitive information processing facilities must be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They must be physically protected from unauthorised access, damage, and interference.
- A staffed reception area or other means to control physical access to the site or building must be in place; access to sites and buildings must be restricted to authorised personnel.

9.1.2 Physical entry controls

- Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access
- The date and time of entry and departure of visitors must be recorded, and all visitors must be supervised unless their access has been previously approved; they must only be granted access for specific, authorised purposes and must be issued with instructions on the security requirements of the area and on emergency procedures.
- Access to areas where sensitive information is processed or stored must be controlled and restricted to authorised persons only; authentication controls, e.g. access control card plus PIN, must be used to authorise and validate all access; an audit trail of all access must be securely maintained;
- All employees, contractors and third party users and all visitors must be required to wear some form of visible identification and must immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
- Third party support service personnel must be granted restricted access to secure areas or sensitive information processing facilities only when required; this access must be authorised and monitored;
- Access rights to secure areas must be regularly reviewed and updated, and revoked when necessary.

9.1.5 Working in secure areas

- Physical protection and guidelines for working in secure areas must be designed and applied.
- Staff must only be aware of the existence of, or activities within, a secure area on a need to know basis;
- Unsupervised working in secure areas must be avoided both for safety reasons and to prevent opportunities for malicious activities;
- Vacant secure areas must be physically locked and periodically checked;
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, must not be allowed, unless authorised;

9.1.6 Public access, delivery, and loading areas

- Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.
- Access to a delivery and loading area from outside of the building must be restricted to identified and authorised personnel;
- The delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;

- The external doors of a delivery and loading area must be secured when the internal doors are opened;
- Incoming material must be registered in accordance with asset management procedures on entry to the site;
- Incoming and outgoing shipments must be physically segregated, where possible.

9.1 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.

9.2.1 Equipment siting and protection

- Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
- Equipment must be sited to minimise unnecessary access into work areas;
- Items requiring special protection must be isolated to reduce the general level of protection required;
- Controls must be adopted to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
- Guidelines for eating, drinking, and smoking in proximity to information processing facilities must be established;
- Environmental conditions, such as temperature and humidity, must be monitored for conditions, which could adversely affect the operation of information processing facilities;
- Lightning protection must be applied to all buildings and lightning protection filters must be fitted to all incoming power and communications lines;
- Equipment processing sensitive information must be protected to minimise the risk of information leakage due to emanation (emitted or radiated).

9.2.2 Supporting utilities

- Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
- All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning must be adequate for the systems they are supporting. Support utilities must be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.
- A suitable electrical supply must be provided that conforms to the equipment manufacturer's specifications.

9.2.6 Secure disposal or re-use of equipment

- All items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
- Devices containing sensitive information must be physically destroyed or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. This information must also be protected (i.e. not lost) as a result of this control.

10. Communications and operations Management

10.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

10.1.1 Documented operating procedures

- Responsibilities and procedures for the management and operation of all information processing facilities must be established. This includes the development of appropriate operating procedures
- Operating procedures must be documented, maintained, and made available to all users who need them.

10.1.3 Segregation of duties

- Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

10.1.4 Separation of development, test, and operational facilities

- Development, test, and operational facilities must be separated, where possible, to reduce the risks of unauthorised access or changes to the operational system.

10.4.1 Controls against malicious code (including viruses)

Objective: To protect the integrity of software and information.

- Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures must be implemented.
- ICT managed equipment must be maintained with the most recent anti-virus vendor signature updates via a centrally managed console. The updates must be automatically distributed, with no manual intervention required by the end user or ICT.

10.5 Backup and Restore

Objective: To maintain the integrity and availability of information and information processing facilities.

- Routine procedures must be established to implement back-ups processes across all ICT managed equipment.
- The backup processes must be thoroughly tested and documented.
- Routine restores of data must be performed to confirm the restore capability.

10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

- Networks must be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

10.6.2 Security of network services

- Security features, service levels, and management requirements of all network services must be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

10.7 Media Handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to operational activities.

- Media must be controlled and physically protected by the support teams.

- Appropriate operating procedures must be established to protect documents, computer media, input/output data and system documentation from unauthorised disclosure, modification, removal, and destruction.

10.7.1 Management of removable media

- There must be procedures in place for the management of removable media.
- Where sensitive classified information is stored on removal media, appropriate controls such as password protection and encryption must be applied at a minimum to protect the information.

10.10 Monitoring

Objective: To detect unauthorised information processing activities where assets are classified as sensitive.

10.10.2 Monitoring system use

- Procedures for monitoring use of information processing facilities must be established and the results of the monitoring activities reviewed regularly.
- The level of monitoring required for individual facilities must be determined by a risk assessment.
- Must comply with all relevant legal requirements applicable to its monitoring activities.

10.10.3 Protection of log information

- Logging facilities and log information must be protected against tampering and unauthorised access.
- Controls must aim to protect against unauthorised changes and operational problems with the logging facility.

10.10.4 Administrator and operations logs

- System administrator and system operator activities must be logged.
- Logs must include:

  a) The time at which an event (success or failure) occurred;

  b) Information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);

  c) Which account and which administrator or operator was involved;

  d) Which processes were involved.
- System administrator and operator logs must be reviewed on a regular basis. Any abnormalities must be reported for further investigations.

10.10.5 Fault Logging

- Faults must be logged, analysed, and appropriate action taken.
- Faults reported by users or by system programs related to problems with information processing or communications systems must be logged. There must be clear rules for handling reported faults including:
- Review of fault logs to ensure that faults have been satisfactorily resolved;
- Review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorised.
- It must be ensured that error logging is enabled, if this system function is available.

10.10.6 Clock synchronisation

- The clocks of all relevant information processing systems within an organisation or security domain must be synchronised with an agreed accurate time source.
- Where a computer or communications device has the capability to operate a real-time clock, this clock must be set to an agreed standard, e.g. Coordinated Universal Time (UTC). As some clocks are known to drift with time, there must be a procedure that checks for and corrects any significant variation.
- The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. Local specifics (e.g. daylight savings) must be taken into account.

11 Access Control

11.1 Operational requirement for access control

Objective: To control access to information.

- Access to information, information processing facilities, and operational processes must be approved on the basis of operational and security requirements by the nominated owner.
- Anonymous access is not permitted to assets classified as sensitive.
- Access control rules and rights for each user or group of users must be clearly stated.

11.2 User Access Management

Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

- Formal procedures must be in place to control the allocation of access rights to information systems and services.
- The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.
- Special attention must be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

11.2.1 User registration

- There must be a formal user registration and de-registration procedure (user registration form) in place for granting and revoking access to all information systems and services.
- The access control procedure for user registration and de-registration must include:
    - Using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs (role based accounts) must only be permitted where they are necessary for operational reasons, and must be approved and documented;
    - Ensuring service providers do not provide access until authorization procedures have been completed;
    - Maintaining a formal record of all persons registered to use the service;
    - Immediately removing or blocking access rights of users who have changed roles or jobs or left the organisation;
    - Periodically checking for, and removing or blocking, redundant user IDs and accounts after inactivity for 90 days, deletion after 180 days;
    - Redundant user IDs are not to be issued to other users.

11.2.2 Privilege Management

- The allocation and use of privileges must be restricted and controlled.
- The principle of least privilege must be applied. Approved access by the asset owner must only be granted if it is deemed necessary to support a legitimate operational requirement.
- Privileges must be assigned to a different user ID from those used for normal operational activity.

11a Password Policy

11.2.3 Password Policy:

- The following controls must be applied:
    - User-level passwords must be kept confidential. If your password has been compromised – change your password immediately.
    - User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
    - Passwords must not be inserted into email messages or other forms of electronic communication.
    - Passwords must never be written down or stored online.
    - Passwords must never be included in scripts.
    - Initial passwords must be change on first time use.
    - Procedures to verify the identity of the requesting a new, replacement or temporary password must be followed by the persons performing the change.
    - Default vendor passwords must be altered following installation of systems or software.
    - Where possible, account must be disabled after 5 unsuccessful login attempts for account that access sensitive information.
    - Where possible, the last 9 passwords must not be re-used.
    - Maintain separate passwords from internal and external system access. For example, do not use your online banking password within the University of Sydney.
    - A keyed hash must be used where available. E.g. SNMP
- All user-level and system-level strong passwords must conform to the following minimum of three of the following criteria, where possible:
    - Contain both upper and lower case characters (e.g., a-z, A-Z);
    - Have digits and punctuation characters as well as letters e.g.,$%^&;
    - Is at least eight characters long;
    - Is not a word in any language, slang, dialect, jargon, etc.
    - Is not based on personal information, names of family, etc.

  Create a strong password that is easy to remember. Think of a phrase that you can easily remember. E.g. "This May Be One Way To Remember" and the password could be: "TmB1w2R!".

11.3 User Responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

- A clear desk and clear screen policy must be implemented to reduce the risk of unauthorised access or damage to papers, media, and information processing facilities for information classified as sensitive.

11.4 Network Access Control

Objective: To prevent unauthorised access to networked services.

- Access to both internal and external networked services must be controlled.

11.4.1 Policy on use of network services

- Users will only be provided with access to the services that they have been specifically authorised to use.

11.4.2 User authentication for external connections

- Appropriate authentication methods are required to control access for remote users.

11.4.3 Equipment identification in networks

- Automatic equipment identification must be considered as a means to authenticate connections from specific locations and equipment.

11.4.4 Remote diagnostic and configuration port protection

- Physical and logical access to diagnostic and configuration ports must be controlled.

11.4.5 Segregation in networks

- Groups of information services, users, and information systems must be segregated on networks <as per the Network Strategy>

11.4.6 Network connection control

- For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications.

11.4.7 Network routing control

- Routing controls are essential to ensure that computer connections and information flows do not breach the access control policy of the business applications.

12. Information Systems Acquisition, Development and Maintenance.

12.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

12.2.1 Input data validation

- Data input to applications must be validated to ensure that this data is correct and appropriate.

12.2.3 Message integrity

- Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and appropriate controls identified and implemented where classified as sensitive.

12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

12.3.2 Key management

- Key management must be in place to support the organisation's use of cryptographic techniques.
- All cryptographic keys must be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorised disclosure. Equipment used to generate, store and archive keys must be physically protected.
- A key management system must be based on an agreed set of standards, procedures, and secure methods for:
- Generating keys for different cryptographic systems and different applications;
- Generating and obtaining public key certificates; distributing keys to intended users, including how keys must be activated when received;
- Storing keys, including how authorised users obtain access to keys;
- Changing or updating keys including rules on when keys must be changed and how this will be done;
- Dealing with compromised keys;
- Revoking keys including how keys must be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys must also be archived);
- Recovering keys that are lost or corrupted as part of operational continuity management, e.g. for recovery of encrypted information;
- Archiving keys, e.g. for information archived or backed up;
- Destroying keys;
- Logging and auditing of key management related activities;
- Proactive renewal of expired keys, prior to expiration date.

12.4 Security of system files

Objective: To ensure the security of system files.

12.4.1 Control of operational software

- There must be procedures in place to control the installation of software on operational systems.

12.4.3 Access control to program source code

- Access to program source code must be restricted.

12.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

12.5.1 Change control procedures

- The implementation of changes must be controlled by the use of ICT change control procedures.

12.5.2 Technical review of applications after operating system changes

- When operating systems are changed, critical applications must be reviewed and tested to ensure there is no adverse impact on organisational operations or security as part of ICT change control process.

12.5.3 Restrictions on changes to software packages

- Modifications to software packages must be discouraged, limited to necessary changes, and all changes must be strictly controlled as part of the ICT change control process.

12.5.5 Outsourced software development

- Outsourced software development must be supervised and monitored by the organisation.

12.6 Technical vulnerability management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities. Technical vulnerability management must be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

12.6.1 Control of technical vulnerabilities

- A centralised vulnerability management process must be established.
- All information about technical vulnerabilities of information systems being used must be obtained from external authorities such as AUSCERT to a central point of control – The ICT Security team.
- Vendor ratings will be adopted.
- The organisation's exposure to such vulnerabilities will be evaluated.
- An agreed timeline must be defined to react to notifications of potentially relevant technical vulnerabilities.
- The appropriate measures in conjunction with the asset owner must be taken to address the associated risk.
- A patch management process must be established, implemented and monitored for all systems, maintaining a minimum patch level of n-1. This process will be managed by the ICT change management process.
- This will include an agreed (with ICT Relationship Managers) patch schedule for all ICT managed servers.

13. Information Security Incident Management

13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

- All employees, contractors and third party users must be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organisational assets. They must report any information security events and weaknesses as quickly as possible to the designated point of contact.

13.1.1 Reporting and management of information security events

- A formal information security event reporting procedure must be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event.
- Responsibilities and procedures must be in place to handle information security events and weaknesses effectively once they have been reported, (as per the ICT Incident Response process).
- The first point of contact will be the ICT Helpdesk for all Information Security related events. Tickets will be generated for the ICT Security team.
- The ICT security team will evaluate the information and determine the appropriate course of action.
- Any non-authorised investigation outside the approval of the ICT Security team will be managed by disciplinary processes as per The Code of Conduct.
- The existing ICT incident management process will be adopted.
- A process of continual improvement will be applied to the response to, monitoring, evaluating, and overall management of information security incidents.
- Where evidence is required, it must be collected to ensure compliance with legal requirements.

14. Business Continuity Management

14.1 Information Security Aspects of business continuity management

Objective: To counteract interruptions to operational activities and to protect critical processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

- A business continuity management process must be implemented to minimise the impact on the organisation and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.
- This process must identify the critical processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.
- The consequences of disasters, security failures, loss of service, and service availability must be subject to a business impact analysis. Business continuity plans must be developed and implemented to ensure timely resumption of essential operations. Information security must be an integral part of the overall business continuity process, and other management processes within the organisation.
- Business continuity management must include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for operational processes is readily available.

15. Compliance

15.3 Information systems audit considerations

Objective: To maximize the effectiveness of and to minimise interference to/from the information systems audit process.

- There must be controls to safeguard operational systems and audit tools during information systems audits.
- Protection is also required to safeguard the integrity and prevent misuse of audit tools.

15.3.2 Protection of information systems audit tools.

- Access to information systems audit tools must be protected to prevent any possible misuse or compromise.
- Access to such applications must be via an authentication process.
- Use of such tools must be authorised by the ICT Security Manager prior to installation/use.

16. Exemptions

For any exemptions to this policy, please complete the Security Exemption form for subsequent review/approval by the ICT Security Manager.

17. Related information

(1) Related University legislation, resolutions, policies and procedures include:

(a) Commonwealth Legislation: Crimes Act 1914, Cybercrime Act 2001, Electronic Transactions Act 1999, Corporations Act 2001, Trade Practices Act 1974, Trade Practices Amendment Act 2001, Sex Discrimination Act 1984, Racial Discrimination Act 1975, and Disability Discrimination Act 1992

(b) NSW Legislation: NSW University of Sydney Act 1989, NSW State Records Act 1998, NSW Privacy and Personal Information Protection Act 1998, NSW Health Records and Information Privacy Act 2002, NSW Freedom of Information Act 1989, NSW Workplace Surveillance Act 2005

(c) Sydney University Policies (http://www.usyd.edu.au/policy), such as:

(i) Code of Conduct – Staff

(ii) Student Code of Conduct

(iii) Use of University Information and Communication Technology Resources (ICT Resources) Policy

(iv) University Privacy Policy

(v) University Web Sites Privacy Statement

(vi) University Recordkeeping Policy

(vii) University Record Keeping Manual

(viii) University Freedom of Information Policy

(ix) Risk Management Policy

18 Procedures

Implementation Action plans:

1. High Level Executive - see Attachment 7 - Seven key implementation activities.docx.
2. Implementation Level Documentation – see Attachment 6 - ICT Information Security Policy Implementation Guide .docx

Administration

1. Background

For consultation and review process – see Attachment 4 - Consolidated feedback log.docx, and who was responsible for developing the policy.

The policy was developed by:

Louise Schuster

Manager, Information Security

Information and Communications Technology

The University of Sydney

2. Policies, procedures etc which are now superseded by this document and its attachments

ICT Information Security Policy at http://www.usyd.edu.au/ict/ policy/ICT-Information-Security-Policy-20061211.pdf

3. Management Responsibility

Bruce Meikle

Chief Information Officer,
Information and Communications Technology
The University of Sydney

4. Implementation Responsibility

Manager, Information Security

Information and Communications Technology

The University of Sydney

5. Dates

Approval (version 1)	
Effect	
Review	
Approval (version 2)	
Effect	

6. Approval

Version 1	
Version 2	

7. Signatures

Approved by:

Name

Dr Michael Spence

Position

Vice-Chancellor and Principal

Date

Signature