

THE UNIVERSITY OF MELBOURNE IT SECURITY POLICY GUIDELINES

EXECUTIVE SUMMARY

This document is written to elaborate on the elements in the IT Security Policy, with the aim of adding practical guidelines to assist personnel in complying with the IT Security Policy. The IT Security Policy is accessible at:

<http://www.infodiv.unimelb.edu.au/it-security/docs/ITSecPol.pdf>

INTENTION OF THIS DOCUMENT

The IT Security Policy is written at a high level in order to cover the essential points and be applicable to the whole University community. The It security policy guidelines add more detail to assist University personnel in the interpretation of the IT Security Policy. It is recognised that a devolved IT environment exists, and departments will differ in the implementation of some IT Security procedures.

This document seeks to strike a balance between being too general and being too specific. To be too general would result in a lack of details, and being too specific would result in the guidelines not being practical or relevant.

ORGANISATION AND PRESENTATION OF THIS DOCUMENT

This document contains the IT Security Policy, divided into its various elements. Each element of the IT Security Policy is contained in a box, and immediately following that are the guidelines. The next element of the IT Security Policy continues on a fresh page.

George Ng
Greg Chenhall
Yalcin Adal
02 Dec 2003

The University of Melbourne

INFORMATION TECHNOLOGY SECURITY POLICY

1 INTRODUCTION

2 POLICIES

2.1 ASSET MANAGEMENT

2.2 EQUIPMENT SECURITY

2.2.1 Secure Disposal

2.2.2 Removal of Property

2.3 ACCESS CONTROL

2.3.1 General

2.3.2 Location of Equipment

2.3.3 Cabling

2.3.4 Network Access

2.3.5 User Authentication

2.4 ENCRYPTION

2.5 MONITORING

2.6 SYSTEM DEVELOPMENT AND MAINTENANCE

2.7 PERSONNEL

2.8 BACKUPS

2.9 WIRELESS NETWORKING

2.10 DIALIN ACCESS

2.11 RISK MANAGEMENT AND BUSINESS CONTINUITY PLANNING

3 RESPONSIBILITIES

3.1 INFORMATION STRATEGY COMMITTEE

3.2 VICE PRINCIPAL (INFORMATION), INFORMATION DIVISION AND THE IT SECURITY
COORDINATOR

3.3 HEADS OF DEPARTMENT AND DEANS

3.4 STAFF

3.5 STUDENTS

3.6 INTERNAL AUDIT

4 BREACHES OF THESE POLICIES

1 INTRODUCTION

This document defines policies of The University of Melbourne to assist in ensuring the security of the University's Information Technology (IT). Security is particularly concerned with the preservation of:

- Confidentiality – ensuring information is accessible only by those authorised to have access,
- Integrity – safeguarding the accuracy and completeness of information and processing methods,
- Availability – ensuring that authorised users have access to information and associated assets when required.

When applying security, some tension between these three considerations can exist, particularly between a need to provide availability and confidentiality.

This document applies in the use of all University of Melbourne IT facilities.

Regulation 8.1R7 defines overall requirements governing the use of IT facilities at the University, see

<http://www.unimelb.edu.au/Statutes/r81r7.html>

This document has been prepared with reference to Australian Standard 17799:2001, and was approved by the Information Strategy Committee on 14 April 2003 with the addition of a section on disposal of media containing information.

2 POLICIES

2.1 ASSET MANAGEMENT

Assets are items of value to the University, and in the context of IT can be equipment, cabling and software (including computer programs, data and files).

The existence, location, value and ownership of assets of significant value must be recorded in an IT Asset register and an annual review conducted to ensure assets are in place.

Significant value is defined to be greater than \$5,000 (as applies to non-attractive Physical Assets in the University Finance Policy and Procedures Manual). Items such as software (developed by or for the University) which the University or owner believes has significant value must be included in IT Asset registers.

2.1a IT ASSET REGISTER

IT assets can be IT-based equipment, components, software and data. Examples include computers, laptops, personal digital assistants, memory sticks, flash ROMs, diskettes, hard disk drives, compact discs, research data, documents, patents, intellectual property, etc.

Information assets can be stored in IT assets. Examples of information assets are patents, intellectual property, and research data.

The purpose of an Asset Register is to account for all items of significant value (ie greater than \$5,000) for the purposes of having a record of:

- a. the owner of the asset

- b. the custodian of the asset
- c. the status of the asset
- d. the value of the asset
- e. the location of the asset

A spreadsheet can be used to create an IT Asset Register noting the value of software developed, and other items of significant value. This information will assist in establishing clear accountability of IT Assets, and assist IT staff in the maintenance of IT Security.

2.1b IT ASSET MANAGEMENT - ANNUAL REVIEW

It is a good practice to conduct an annual review of all items in the Asset Register. Keeping the IT Asset Register updated is a task that should be done promptly whenever there are changes to be updated, so that the IT Asset Register contains an accurate record of IT Assets at all times. The annual review is not the time to do the updating.

The purpose of the annual review is to verify the accuracy of the IT Asset Register. A complete check, including physical inspection, is best. Where resources are insufficient to do a complete check, a random sample across the various categories of IT Assets should be checked for accuracy against the IT Asset Register.

Previous IT Asset Registers should be preserved so that a history of an asset can be tracked through the various IT Asset Registers over a period of time.

Information on updating Asset Registers can be found at:
<http://www.unimelb.edu.au/finance/authofficers/18.html>

2.2 EQUIPMENT SECURITY

2.2.1 Secure Disposal

Valuable information could be compromised accidentally through the disposal or redeployment of equipment which contains media or via the disposal of media itself. Media in this context includes items such as hard disks, tapes, CDs as well as other removable or static data storage devices.

When equipment containing media, or media itself, is to be disposed or re-deployed any sensitive information must be removed in such a way as to make the data unrecoverable. Such media should be overwritten by tools designed to make the data unrecoverable, or the media itself must be physically destroyed to make the data unreadable.

2.2.1a SECURE DISPOSAL

Before any IT equipment is disposed of, steps should be taken to remove all sensitive data from storage systems associated with that equipment. Depending on the degree of sensitivity, the storage devices should be:

- Permanently erased (including erasing from the “Recycle Bin” or similar facility)
- Reformatted
- Overwritten one or more times
- Degaussed
- Physically destroyed beyond any means for the resident data to be retrieved

It is best if the Head of Department, or Head of Department delegate or the IT Security Nominee determines the measures required to prevent disclosure of data, which relate to its sensitivity and ability to disclose confidential or personal information.

2.2.1b REDEPLOYMENT

When any equipment is to be redeployed, steps should be taken to remove any data that is not relevant to the next custodian of the computer equipment. Depending on the sensitivity of the resident data, the existing storage device should be:

- Permanently erased (including erasing from the “Recycle Bin” or similar facility)
- Reformatted
- Overwritten one or more times
- Degaussed
- Disposed of (procedures on secure disposal apply), and a new storage device issued.

2.2.2 Removal of Property

Equipment with stored information of significant value should not be taken from secure areas without authorization. Where equipment containing sensitive information is to be taken off-site for repair, repairers should be trusted employees of the University or third-parties which guarantee the confidential handling of University information.

2.2.2a REMOVAL OF PROPERTY

Custodians of IT equipment should ensure that authorisation is given for equipment to be removed. The custody of the equipment after it is removed is to be established, and noted in the IT Asset Register. The record should contain, where applicable, at least the following information:

- a. University management staff authorising the removal of the equipment
- b. reason(s) for the removal
- c. full name and contact information of the new custodian of the equipment
- d. date and time of removal of equipment
- e. date and time of return of equipment

Consideration should be given to the security of any data or information stored on the equipment. Where applicable, the next custodian of the equipment should undertake to preserve the confidentiality of all information stored on the IT equipment. If necessary, take a verified back up of the data then store the backup media securely. Remove the data irretrievably from the equipment before custody of the equipment is transferred.

Upon the return of that equipment, it should be verified for any IT security compromise before being put into the normal operating environment.

2.2.2b REMOVAL FOR MAINTENANCE

Equipment that undergoes maintenance should have sensitive data removed, such that the data is not retrievable by any other party. This will safeguard the data from being inadvertently lost during maintenance activities, and also prevent disclosure of sensitive data. The sensitive data should be backed up and verified, then stored in a secure location.

Where applicable, the maintenance personnel working on the IT equipment should undertake to preserve the confidentiality of all information stored on the IT equipment.

An entry should be made in the IT Asset Register to indicate the maintenance activity on the IT equipment. The record should contain, where applicable, at least the following information:

- University management staff authorising the removal of the equipment for maintenance
- nature of maintenance
- full name and contact information of the new custodian of the equipment
- date and time of removal of equipment

- date and time of return of equipment

Upon the return of that equipment, it should be verified for any IT security compromise before being put into the normal operating environment.

External links with information on security of information on storage media can be found at:

<http://www.dsd.gov.au/infosec/acsi33/HB6.html>

<http://computer.org/security/v1n1/garfinkel.htm>

2.3 ACCESS CONTROL

2.3.1 General

Unless purchased specifically for general access by the public, access to University IT facilities must be restricted by

- location of the facility and/or
- explicit notice stating access conditions and/or
- software which prevents unauthorised access.

2.3.1a EQUIPMENT PURCHASED FOR USE IN PUBLIC

IT Equipment purchased for public use, such as information kiosk, library terminals, etc should be easily accessible by the public, but appropriately secured against unauthorised removal, damage or misuse. Some measures to preserve the availability of the IT equipment for the public include:

- Secure housing
- Restricting access to the internal components of the equipment
- Restricting access to the electricity supply, communication cables, etc
- Restricting access to functions and software that are not required for purpose of providing the IT equipment for public use.

Prominent notices should be placed at the equipment stating conditions for access, including IT Security aspects. The conditions for access should comply with the provision of the service as advertised to University personnel.

It is best practice to have remote management of the computers to update software for security vulnerabilities or to re-install a predefined computer image, including the Operating System and Applications.

Some pointers on restricting access can be found at:

<http://www.dsd.gov.au/infosec/acsi33/HB7.html>

2.1.3b EQUIPMENT PURCHASED FOR USE BY UNIVERSITY PERSONNEL

IT Equipment purchased for use only by University personnel should have its use restricted by one or more of the following measures:

- The equipment should be made available at the location as published to University personnel. Measures should be taken to secure the equipment from unauthorised removal, like locking the office. Steps to preserve the availability and functioning of the equipment should also be taken, especially in cases where several persons may use the same equipment.
- Software should be implemented on the equipment to prevent unauthorised access.
- Password protected screensavers should be used.

Regulation 8.1.R7 Under Statute 8.1 applies and can be accessed at:
<http://www.unimelb.edu.au/Statutes/r81r7.html>

2.3.2 Location of Equipment

Equipment on campus must be located in a lockable and/or appropriately monitored location. Consideration must be given to the reliability of the electrical power supply, the need for air conditioning, potential contamination (e.g. from dust particles) and the likelihood of flooding. Staff assigned to take equipment off campus (e.g. a portable computer) must take appropriate care to safeguard it.

2.3.2a LOCATION OF EQUIPMENT

The location of IT equipment should be reflected accurately in the IT Asset Register (see section 2.1a). Changes in the location of equipment for extended periods of time should be recorded in the IT Asset Register, such as when the equipment is re-deployed or sent for maintenance (see section 2.2.1b and 2.2.2a)

2.3.2b PHYSICAL SECURITY

All IT equipment should be physically secured in a manner relevant to the environment in which it is being used.

IT equipment in public access areas and laboratories should be physically locked down to prevent it being removed by unauthorised persons. Physical security of equipment in this environment should also include consideration of access to internal components, electricity supply, communication cables, etc.

IT equipment in private areas should be physically secured by locking the room after hours or when staff are not present for extended periods of time.

Regulation 8.1.R8 Under Statute 8.1 has some information on physical security:
<http://www.unimelb.edu.au/Statutes/r81r7.html>

2.3.2c OPERATING ENVIRONMENT

IT equipment should be used and stored in accordance with the stipulated operating environmental conditions.

Consideration should be given to the ambient conditions, including temperature, humidity, quality of electrical power supply during and after office hours, over weekends, and extended holidays.

For important or sensitive IT equipment, it is recommended that backup power such as an Uninterruptible Power Supply (UPS) unit with graceful shutdown facilities be implemented to safeguard the equipment and the information stored on it. The UPS should be able as a minimum to provide a good quality of electrical power at all times, and initiate a graceful shutdown to avoid loss of data.

Following are some links to data centres with specifications on controlling the operating environment for IT equipment:

<http://www.westnet.com.au/products/hosting/colocate/>

http://www.hosting365.ie/html/infra_data.htm

2.3.2d MOBILE EQUIPMENT

Mobile equipment should be physically secured at all times, to prevent unauthorised removal. When the mobile equipment is openly visible, it should be locked to the table or an immovable fixture. When in transit, it should be carried in an appropriate carrying case. If during transportation, the mobile equipment is left in a vehicle for extended periods, it should be stored out of sight before arrival at the destination. Whenever feasible, the mobile equipment should be with the custodian, and not, for example, checked in as luggage on an aeroplane.

When mobile equipment is not being used, for example, after business hours or for extended periods of time, the equipment should be kept under lock and key, preferably out of sight.

2.3.3 Cabling

Cabling must be kept secure by hiding major cable routes and by requiring key access to cabling locations except where workstations are designed to connect to the cabling systems. The Information Division defines detailed requirements for the installation of cabling; see <http://www-networks.its.unimelb.edu.au/Standards/WiringStandards.html>

2.3.3a CABLING

Cabling used for the transmission of communication signals is an important component in IT Security, because this is the conduit through which information flows. Cables could be tapped for eavesdropping or severed to disrupt communications.

Cables on University property should be concealed and not accessible by unauthorised personnel. This should be observed for as much of the cable run as possible until the termination point at the faceplate.

Network equipment and patch panels should be secured by lock and key. Equipment cabinets and patch panels should be in a room dedicated for this purpose. The condition of the operating environment should be appropriate for the equipment. (Section 2.3.2c)

Detailed requirements on cabling can be found at:

<http://www-networks.its.unimelb.edu.au/Standards/WiringStandards.html>

<http://www.dsd.gov.au/infosec/acsi33/HB5.html>

2.3.4 Network Access

Traffic on the University Network must be segregated to minimise traffic levels and limit transmissions to appropriate paths. This provides an inherent level of security. Certain external addresses, namely those which are considered or known to send generally undesirable transmissions, are to be blocked from access to the University Network. The Information Division is responsible for the management and configuration of central facilities to do this. A primary location for such a facility is the University's connection to the Internet but similar techniques may be applied restricting access to individual servers/services.

2.3.4a NETWORK ACCESS

The use of broadcast transmission of communications should be avoided to the maximum limit feasible. Network equipment working on multipoint broadcast domains, such as hubs and co-axial cable should not be used, unless there are very special constraints. The use of such technologies should be approved by the relevant IT Security Nominee.

The broadcast nature of certain networks, for example, wireless networking, is a property of existing radio technology, and appropriate measures such as encryption should be implemented where appropriate to preserve IT Security when using these services.

In the interest of protecting IT equipment in the University, the Information Division may implement blocks on specific applications where possible, on known servers housing security threats. There may also be a requirement to block harmful traffic inbound to or outbound from the University.

Following are links with information on this element of IT Security:

<http://www.dsd.gov.au/infosec/acsi33/HB8.html>

<http://www.auscert.org.au/render.html?it=2249>

2.3.5 User Authentication

Access to sensitive IT services shall only be through approved accounts which include a logon process defining the user and the declaration of a secret password that conforms to defined rules. Rules for passwords are contained at

<https://accounts.unimelb.edu.au/manage/passwords/index.html>

Logs shall be kept of access by the operators of such IT facilities for investigation of security incidents.

2.3.5a USER AUTHENTICATION

Access to sensitive information or sensitive IT services should be provided through accounts that are approved by management responsible for the service. There should be a mandatory login process before users are allowed access to the system. The rights and privileges of the user accounts should be the minimum required for the user to carry out his/her tasks. Logging of each user's activity on the system should be kept for evidence to assist in investigations in the event of an IT Security incident.

The following two links provide information about choosing effective passwords:

<http://www.unimelb.edu.au/Statutes/r81r7.html>

<http://accounts.unimelb.edu.au/passwords.html>

<http://www.cert.org/homeusers/HomeComputerSecurity/#6>

2.4 ENCRYPTION

Encryption must be applied to highly sensitive information communications. The Information Division is able to provide advice on such technology to departments concerned about the monitoring of transmissions, and this is a function of the IT Security Coordinator.

2.4a SENSITIVE INFORMATION

If the sensitive information is stored on a device, additional measures should be taken to safeguard the sensitive information from being accessed or the device being removed by unauthorised persons. Sensitive data should be irretrievably removed from the storage device when it is no longer required.

Sensitive information should be encrypted before communication. This applies to all communication channels for the University network. Examples include communication of information via:

- the University local area network
- the Internet
- a dial up connection
- access when using another person's computer,
- physically transferable devices (eg floppy disks, external storage media, mobile equipment, etc)

The University has implemented a VPN solution to facilitate encrypted communication. Information on this service can be found at:

<http://www.infodiv.unimelb.edu.au/vpn/>

2.5 MONITORING

The Information Division is responsible for the monitoring of University Network communications to and from the Internet for accounting purposes. It must also monitor communications to and from the Internet to try to detect attacks and may halt transmissions it believes are suspicious.

Departments and others must not monitor communications unless the action accords with Regulation 8.1R7. If any doubt exists, the IT Security Coordinator must be requested to have the matter clarified.

2.5a MONITORING

The Information Division monitors IT communications for accounting and for IT Security purposes. Uses for the information gathered include notifying departments which have a sudden spike in traffic, verifying reports that computers in the University are engaging in inappropriate behaviour, and collecting evidence for investigations into IT Security incidents. The information gathered may be used for internal investigations or as required by government agencies such as the Police.

Departments monitoring their own IT communications should do so within the requirements in Regulation 8.1R7, which can be accessed at:
<http://www.unimelb.edu.au/Statutes/r81r7.html>

2.6 SYSTEM DEVELOPMENT AND MAINTENANCE

The University's procurement requirements are at:

<http://www.unimelb.edu.au/FinPPM/FPP0home.htm>

Consideration shall be given to the use of formal testing and change control procedures and the provision of integrity checking and logs to provide audit trails.

Software developed to manage financial, staff and student records and similarly critical functions must be developed by one team, and implemented (i.e. made live) by another team. The implementation team (i) must ensure the code has been thoroughly tested to meet its purpose and (ii) confirm the code only performs the actions for which it was designed.

Development staff must not have access to change the production environment.

2.6a SYSTEM DEVELOPMENT AND MAINTENANCE

IT Security should be considered and included in the system during the development phase. This will ensure that security is embedded and enforced to protect the system, and not added in as an afterthought in an ineffective or inefficient manner.

During system development, consideration should be given to whether Internet access is required. If it is not required, the system should not allow or accept communication with the Internet. The Privacy Act and the level of sensitivity of data should also be considered, and appropriate controls built into the system to adequately handle the information it will process and handle. Default passwords should be changed, and a security audit should be planned for.

2.6b PROCUREMENT REQUIREMENTS

The development and maintenance of systems may involve procurement activities. The Financial Operations Department provides information on finance and accounting matters. This department undertakes policy advice, financial management and accounting services for the University.

The Finance Policy and Procedures Manual can be accessed at:

<http://www.unimelb.edu.au/FinPPM/FinPPM-Themis.pdf>

2.6c SEPARATION OF DUTIES

Separation of duties reduces the risk from errors or illicit activities, whether intentional or accidental. This is achieved by dividing critical tasks into independent sub-tasks which are performed by different personnel. This method thus implements checks and balances, avoiding an error to be carried out from the concept to the implementation of the task.

Requirements include:

- Developer(s) should not have access to the production environment
- Software should be tested by suitably qualified personnel other than the developer(s).
- System Administrators should not perform the role of a System Operator and vice-versa.

Job rotation should be implemented. This scheme will ensure that there is more than one person able to perform any task, and facilitates the detection of errors by another person, which usually is unnoticed by the person performing the task.

2.6d FORMAL METHODOLOGY

Systems development work should be governed by an industry accepted formal methodology. The formal methodology should prescribe adequate measures for:

- documentation
- change control
- testing
- software design
- maintenance
- checks and approval processes

2.7 PERSONNEL

University requirements for recruiting staff are contained at:

<http://www.unimelb.edu.au/ppp/docs/2.html#2.1>

Care must be taken to ensure Visitors and Contractors to the University do not compromise IT security.

2.7a PERSONNEL - RECRUITING STAFF

The Human Resources Department has created a Personnel Policy and Procedures Manual. With the aim of recruiting the best staff for the University, and upholding fairness and openness, a part of the Personnel Policy and Procedures Manual outlines the requirements for the process of recruiting staff. This document can be accessed at:

<http://www.unimelb.edu.au/ppp/docs/2.html>

Recruiting appropriate staff can help to minimise the possibility of IT Security incidents arising from staff actions.

2.7b PERSONNEL - VISITORS AND CONTRACTORS

One or more members of University staff should ensure that visitors and contractors observe IT Security requirements when using the University's IT assets. The University staff should ensure that:

- resources allocated to the visitors and contractors are recorded in the IT Asset Register. The entry should include as a minimum:
 - the unique identifier of the equipment (eg asset tag, serial number, etc)
 - the "start" and "end" dates and times of use of equipment
 - the name and contact information of the person using the equipment
 - the location(s) where the equipment is used
 - other useful information (eg IP address, account name, etc)
- ensuring that updated, live and accepted anti-virus software is used on computers
- ensuring that the computer has the latest patches installed
- ensuring that the visitors and contractors are aware of the University's IT Security Policy and Regulations
- ensuring that the visitors and contractors do not remove, transmit or copy any IT assets, tangible or intangible from the University without authorisation.

2.8 BACKUPS

Important software and data must be backed up and the backups securely stored away from the production facility. Periodic tests must be conducted to ensure the backups can be read. The Information Division is able to provide advice on appropriate backup strategies.

2.8a BACKUPS - TESTING

Backup media should be regularly tested to verify the ability to restore data. The frequency of this testing should be determined by the IT Security Nominee. The test should also review the documentation, procedures and personnel involved in the backup and restoration processes.

2.9 WIRELESS NETWORKING

Wireless computer networks can be particularly insecure because of the ease with which some wireless transmissions can be monitored. Wireless networks must not be used for the transmission of confidential information, unless assurance can be obtained of the encryption and security of transmissions. This applies to use on University campuses and at external locations. The Information Division is able to provide advice in such matters.

2.9a WIRELESS NETWORKING - ASSURANCE OF SECURITY

In cases where services hosted by the department or faculty involve the communication of sensitive information over the wireless network, the IT Security Nominee is responsible for ensuring that there are adequate security measures to protect the sensitive information. These measures may include authentication, encryption and access control.

2.10 DIALIN ACCESS

Encrypted communication must be used to assist secure transmission of sensitive information over dialin services or from the Internet. Virtual Private Network technology and services facilitate encrypting the transmission of sensitive information.

2.10a DIAL-IN ACCESS - COMMUNICATION OF SENSITIVE INFORMATION

When using the University's dial-in access service, the user should have systems in place to ensure that the computer is not infected with a virus or Trojan. These can lead to a compromise of security when the attacker "piggy backs" on the legitimate connection made by the user.

At all times, encryption should be in force before communicating sensitive information, especially when using the dial-in access service.

The University has implemented a VPN solution to facilitate encrypted communication. Information on this service can be found at:

<http://www.infodiv.unimelb.edu.au/vpn/>

2.11 RISK MANAGEMENT AND BUSINESS CONTINUITY PLANNING

For each major IT-based service, an assessment of risks to that service must be conducted and documented by the area managing it. For critical services, detailed consideration must be given to the provision of redundant facilities and fail-safe operations. A Business Continuity Plan must be documented which defines procedures to be followed in the event of a serious or catastrophic fault. These documents are required to be reviewed annually. In general, the application of security to any particular system or process will be in accordance with the level of risk.

2.11a ANNUAL REVIEW OF RISK ASSESSMENT AND BUSINESS CONTINUITY PLANNING

The risk assessment and business continuity plan should be reviewed annually. Tasks within this review would be to make updates, especially identifying new risks that may have emerged or have been created when changes have occurred.

The history of changes should be tracked, in order to provide historical information so that trends can be analysed.

3 RESPONSIBILITIES

3.1 INFORMATION STRATEGY COMMITTEE

The Information Strategy Committee is responsible for specifying policies and procedures designed to ensure IT at the University is appropriately secure.

3.2 VICE PRINCIPAL (INFORMATION), INFORMATION DIVISION AND THE IT SECURITY COORDINATOR

The Vice Principal (Information) heads the Information Division. The Information Division's responsibilities include:

- the development and operation of a number of IT services used throughout the University,
- the provision of a number of computer systems generally available to students and staff of the University,
- the development and operation of facilities interconnecting department Local Area Networks and providing connectivity between campuses and the Internet,
- the development and provision of a number of University-wide network based services.

The Vice Principal (Information) or nominee is responsible for appointing someone specifically responsible for the security of these services.

The Vice Principal (Information) or nominee is responsible for appointing an IT Security Coordinator with the following specific responsibilities:

- (1) Coordinating and providing training programmes (including courses, seminars and text) in IT security and risk analysis.
- (2) Determining good practices in IT security.
- (3) Responding to incident reports and coordinating corrective action as necessary.
- (4) Distributing security alerts received from vendors and security agencies (such as AusCERT) as appropriate and necessary.
- (5) Undertaking Risk Assessments and Business Continuity Planning for important central services.
- (6) Defining standards and guidelines for the secure operation of Local Area Networks and computing systems in departments, including the definition of anti-virus software to be deployed on University work stations.
- (7) Liaising with external security organisations such as AusCERT and the police.

Note:

No guidelines are given for the above two sections of the IT Security Policy as it is not necessary.

3.3 HEADS OF DEPARTMENT and DEANS

Heads of Departments are responsible for the security of the IT facilities in their department. Deans are responsible for the security of IT facilities operated at the faculty level. In general it is expected they will appoint someone to carry out duties consistent with policies contained herein. These duties must be included in that person's Position Description. The name and contact details of the person must be notified to the Information Division, and in particular to the IT Security Coordinator.

Responsibilities include:

- (1) The secure configuration of computers purchased by their department (or faculty) in areas available for use by students and the provision of explicit notices stating conditions of use of those computers.
- (2) The secure configuration, consistent with these policies, of servers operated.
- (3) The provision of anti-virus software for computers used by staff, visitors and contractors.
- (4) Ensuring a register is kept of valuable IT assets in their department or faculty.
- (5) Preparing Risk Assessments and Business Continuity Planning for their IT facilities.

Note:

Appreciation is expressed to Yalcin Adal, who wrote the following section on It security policy guidelines for Heads of Department and Deans.

Guidelines for Heads of Department and Deans

	Guideline	Further explanation and examples
1. GENERAL	Deans and Heads of Department are asked to forward the contact information of their appointed IT Security Nominee to the Information Division's IT Security Coordinator (Mr. George Ng)	1.1 IT Security Nominee Contact details
1.2 IT Security for Computers	<p>IT security is the process of preventing and detecting intrusions into the computer system. Security measures help to keep intruders from accessing any part of the computer system. Detection helps to determine whether or not someone attempted to break in, whether or not there was success by the would be intruder.</p> <p>Desktop and laptop computers used by students of the Faculty or Department can be secured using documented security information guides.</p> <p>Computers include the operating systems Windows 95/98, 2000 Professional, Apple Macintosh, and Linux Workstations</p>	<p>1.2.1 Fundamental IT Security Steps</p> <p>1.2.2 Secure Configuration of Student Computers</p> <p>1.2.3 Windows 2000 Professional Computer Security</p> <p>1.2.4 Linux Workstation Security</p>
1.3 Secure Configuration of Computer Servers	<p>Computer Servers in Faculties and Departments are a central and valuable part of the IT Infrastructure for servicing staff, students and users.</p> <p>Servers administered by authorized staff members and students of the Faculty and Department can be fundamentally secured using documented secure configuration guides. Generally servers need to be up-to-date with the latest patches, unnecessary services disabled, and logs managed. Recovery from computer security incidents is an important part of ensuring the integrity of facilities.</p> <p>Operating systems can include Windows, UNIX, Linux and</p>	<p>1.3.1 Keeping Windows 2000 and NT4 Servers Up-to-date</p> <p>1.3.2 Windows 2000 and NT Configuration</p> <p>1.3.3 UNIX Server Configuration</p> <p>1.3.4 Securing Linux Servers</p> <p>1.3.5 Securing Mac OS X Servers</p> <p>1.3.6 Steps for recovery for UNIX and NT from compromise</p>

	Macintosh.	
1.4 Viruses and Unwanted E-mail	<p>Computer viruses are a wide spread problem. They spread by floppy disk (and other media), e-mail and Internet.</p> <p>There are software products known as Anti-virus packages, which defend against computer viruses/worms. The University has bulk licensed anti-virus packages for Windows and Macintosh.</p> <p>Anti-virus packages are to be provided to staff, visitors and contractors to protect against possible virus infections and conform to license agreements.</p> <p>Viruses in the majority of cases affect Windows computers, however they are known to affect Macintosh and UNIX systems as well.</p>	<p>1.4.1 Anti-Virus Packages for Windows and Macintosh</p> <p>1.4.2 Use the Recommended E-mail Client</p> <p>1.4.3 Anti-Spam Filtering</p>
2. ASSET MANAGEMENT	<p>Asset management is necessary to control inventory that identifies information technology assets. An IT Asset Register will assist in this.</p> <p>An IT Asset Register will include the existence, location, value and ownership of an asset of significant value (> \$5000). IT assets include physical, software, and information (data and files) assets. IT Asset Registers should be reviewed and updated where appropriate annually.</p>	2.1 IT Asset Register
3. RISK ASSESSMENT	<p>Risk management is recognized as an integral part of good management practice. It is a process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making. Risk Assessment for every IT-based service by managing area is advisable.</p>	<p>3.1 IT Risk Points</p> <p>3.2 IT Risk Definitions</p> <p>3.3 Risk Register Sample</p>
4. BUSINESS CONTINUITY PLANNING	<p>Business Continuity Planning should be reviewed annually, where disaster recovery documents and plans are</p>	<p>4.1 Back-up Guidelines</p> <p>4.1 IT Disaster Recovery Plans include;</p>

	<p>written for critical areas that flow from the risk register. If for instance your department operates its own Learning Management System for students, then the operation of that is likely to be critical for the business of your area.</p> <p>Key aspects of backups are to keep backup media secure at all times, do not allow unauthorised access to backup media or drives, verify backups and do regular restorations as part of media and procedure checks and destroy compromised backups after a break-in.</p>	<ul style="list-style-type: none"> • Event Log • Recovery Plan • Restoration Procedures • Contact Details of key staff and contractors • Inventories • Testing and Review
--	---	---

1. GENERAL

1.1 IT Security Nominee Contact details

In the event the Information Division and the IT Security Coordinator in particular are in receipt of vulnerability and IT security alerts, the University IT Security Coordinator will require a contact point in departments and faculties so appropriate notification and subsequent action can be taken. The contact details required for an IT Security Nominee are;

- the **Physical address** at University,
- a direct **Telephone number**,
- **Mobile phone number**, and
- **E-mail address**.

1.2 IT Security for Computers

Guidelines to assist Heads of Departments and Deans in meeting their responsibilities in securing computers can be found here.

1.2.1 Fundamental IT Security Steps

There are essential features for securing computers in general (desktop workstations and/or servers) that are not operating systems specific. These are;

- Strong passwords
- Keeping computers up-to-date with the latest patches, hotfixes and/or service packs
- Disable unnecessary services
- Monitor Logs
- Back-up files
- Use screen savers

1.2.1.1 Strong passwords

The password guidelines for keeping passwords secure can be found here;

<http://accounts.unimelb.edu.au/passwords.html>

Passwords should not be shared and students should never give anyone else their password. Passwords should be changed after any known IT security breach in the local area or otherwise with moderate frequency (at least once per year).

1.2.1.2 Keeping computers up-to-date

Timely computer software and operating updates are critical in ensuring the security of computers.

For *Windows 95*

- Go to <http://www.microsoft.com/windows95/>
- Select "Downloads" install patches under the "Critical Updates" and "Recommended Updates" sections.

For *Windows 98*

- Use the Microsoft Windows Update, which is part of the Start menu.

For *Microsoft Office*

- Go to <http://officeupdate.microsoft.com>

For *Internet Explorer*

- Got to <http://www.microsoft.com/windows/ie/security>

For *Netscape*

- If you are using Navigator 4.02 or higher, you can use the **SmartUpdate**.
- Go to the Help menu and then select Software Updates.
- Also review the information about security available under the Help menu.

For *Mac OS X*

- Go to <http://www.infodiv.unimelb.edu.au/it-security/macosexeasy.html>
And http://www.apple.com/support/security/security_updates.html

For *UNIX* and *Linux*

- Go to <http://www.infodiv.unimelb.edu.au/it-security/secunix.html>

It is advisable to check security issues monthly. Some operating systems (Windows, Linux and Mac OS X) and applications (Internet Explorer, Netscape) can be set to automatically check for updates.

1.2.1.3 Disable Unnecessary Services

Network services may run on computers that are not required for departmental or faculty needs and therefore should be disabled. Knowing and willing computer hackers and/or viruses and worms can exploit these services. This can be the result of default system installations and usually include such services as ftp, rpc, telnet and http (web).

1.2.1.4 Monitor Logs

Logging of events on the computer or network provides system, event and date time information. Such information is extremely useful in understanding normal and unusual events, in particular those concerning unauthorised connections and security issues. Daily and weekly monitoring of logs for computer systems is recommended.

1.2.1.5 Back-up files

Good back-up procedures will involve saving files as work progresses. This can be automated as work is produced and also more comprehensive back-ups to file servers on the network. This acts as protection whether there is an IT security incident, a power failure on the computer, or a system failure. Back-ups should be tested by retrieving and restoring to assure it works.

1.2.1.7 Use a screen saver

Use screen saver capabilities of computers to limit access to files. This can be password-protected whenever a computer is left unattended. Don't use screen savers downloaded from the Internet and unknown sources.

1.2.2 Secure Configuration of Student Computers

Computers purchased by departments (or faculty) for the provision of students are advised to use the Fundamental IT Security Steps as outlined in Sec 1.2.1 in addition to that outlined in the coming section.

1.2.2.1 Conditions of use

An explicit notice(s) stating the conditions of use is to be displayed in areas where computers are made available for students. Students should be made aware of the University IT security policy and that breaches may lead to disciplinary measures. In general the principles of IT security should be noted namely confidentiality, integrity and availability of information and computers. These principles ensure the privacy and protection of data, and ensure that resources are available when needed.

1.2.2.2 Physical Security

Students are to be advised to keep their mobile phone, personal organizers, and laptop secure. These items become particularly important from an IT point of view if confidential information and passwords are stored on them.

Students working from information processing areas or offices in the University can purchase a Kensington lock, which is specially designed for laptops and are to be firmly attached to the wall or around a table. Offices should be locked when unattended.

1.2.2.3 Protection against viruses

Viruses tend to exploit security holes in Microsoft Applications i.e. Microsoft Office, Outlook Express, Microsoft Outlook, and Internet Explorer and should be kept up to date with the latest security patches.

Ensure the latest McAfee Virus Scan software for PC and Virex for Macintosh is installed and it is set to automatically update. Note that if anti-virus software is in the middle of a virus scan this should not be cancelled. Guidance for students for configuration in the University setting can be found here;

<http://www.infodiv.unimelb.edu.au/compss/infosheets/virus.html>

1.2.2.4 E-mail handling

Students should be cautious of e-mail sent to them from unknown sources, and particularly when there are attachments involved. If an attachment has been sent from an unknown source, students should verify the source immediately and never open the attachment directly.

Suspicious file extensions include .VBS, .LNK, SHS, EXE, SCR, CHM, COM and BAT. For good practice, students should not send .exe files attached to e-mails. This prompts users to open, launch or execute the attachment. A recommended procedure is to put the file on a server and e-mail the hyperlink for download. Guidance for students for using FTP programs (Fetch and WS_FTP) can be found here;

<http://www.infodiv.unimelb.edu.au/compss/infosheets/ftp.html>

1.2.2.5 WebPage Browser

Student computers should keep up-to-date with the latest patches, hot fixes and service packs for Microsoft Internet Explorer, Netscape Browser and e-mail client.

1.2.3 Windows 2000 Professional Computer Security

Student computers with *Windows 2000 Professional* installed on machines should be configured using the following guides to secure their systems;

1.2.3.1 Hardening the various settings

Settings to harden on Windows 2000 computers include;

- Password policies (only apply to local passwords!)
- Account lockout policies
- Audit settings
- User right assignments
- Security options
- Settings for Event logs
- Restricted groups
- System services
- Registry
- File system

1.2.3.2 Keep operating systems up to date

Keep Windows 2000 Professional workstations (SP2) or XP up-to-date with respect to service packs and patches, which includes those for the operating system, and for applications. Workstations can be set to use the Software Update Service (SUS) with a local mirror on campus at id-sus.unimelb.edu.au.

For information go to; \\dc5\Windows 2000\Utilities\Windows Update Client

1.2.4 Linux Workstation Security

In the provision of Linux computer workstations for students, students are advised to use the Fundamental IT Security Steps as outlined in Sec 1.2.1 in addition to that outlined in the coming section. Linux machines should be maintained and secured by trained and authorized staff. The range of Linux variants supported for workstations should be restricted to a manageable level for secure use. Authorised staff should consider pre-configuration to improve security.

1.3 Secure Configuration of Computer Servers

1.3.1 Keeping Windows 2000 and NT4 Servers Up-to-date

Some major security vulnerabilities in Windows 2000 Servers can be augmented by keeping up-to-date with the latest patches. Windows 2000 Servers can use the web based Windows Update system to apply patches and avoid some potential security issues. A short-cut can be found on the Start Menu of on Windows 2000 Servers and administered to for updates individually from each machine. NT4 are to be kept similarly up-to-date and the Windows Update system provides this functionality, in a similar way to that for Windows 2000 Servers.

1.3.2 Windows 2000 and NT4 Configuration

In addition to that outlined in Sec 1.2.1 Fundamental IT Security Steps, Windows 2000 and NT servers should be secure before connecting to the network and the following given regard;

1.3.2.1 Minimum Installation

The minimum installation for Windows 2000 Server or NT 4.0 includes the latest Service Packs, recommended patches and relevant security Hotfixes released by Microsoft.

1.3.2.2 Computer Virus Prevention

Ensure the latest McAfee Virus Scan software for servers is installed and it is set to automatically update.

1.3.2.3 Network Service Filters

Network service filters and Access Control Lists should be set up to grant or deny access to network services and prevent unauthorized activity.

1.3.2.4 Secure Connections

Secure connections to servers should use SSH to authenticate. Telnet should be disabled.

1.3.2.5 Password Construct Rules

Passwords for servers should consider password aging, minimum password length, uniqueness, and lockout features.

1.3.2.6 File System

The file system should always use NTFS. Share access control lists can also be used where appropriate.

1.3.2.7 Registry settings

Registry settings as recommended by AusCERT can be used as guide;

<http://www.auscert.org.au/render.html?it=1970&cid=1920>

1.3.2.8 Access Control Lists

Access control lists as recommended by AusCERT can be used;

<http://www.auscert.org.au/render.html?it=1970&cid=1920>

1.3.2.9 Audit Logging

Enable audit logging and monitor through Event Viewer for users, files and directories and the registry.

1.3.2.10 Other security includes appropriate recovery procedures in case of compromise (see below 1.3.6).

1.3.3 UNIX Server Configuration

In addition to that outlined in Sec 1.2.1 Fundamental IT Security Steps, UNIX systems should be secure before connecting to the network and the following given regard;

1.3.3.1 Patches

Patches are required for UNIX Servers to fix security vulnerabilities. Patches should be stored to CD or on an isolated file server and checked for integrity (e.g. verify the digital signature). Details for obtaining patches for particular operating systems may be found on the IT security support webpages;

<http://www.infodiv.unimelb.edu.au/it-security/secunix.html>

1.3.3.2 Disable Unnecessary Services

Network services may run on UNIX servers however are not required for departmental or faculty needs and therefore should be disabled. This is a result of default system installations. Some unnecessary services on a particular UNIX server can be ftp, finger and rpc.

1.3.3.3 Log Management

Administration of UNIX servers should consider monitoring of standard log files (such as Syslog) and use programs (such as Swatch) to assist in providing overall data of system activity.

1.3.3.4 Network Service Filters

Network service filters (such as TCP wrappers) or access control lists should be set up to grant or deny access to network services and prevent unauthorized activity.

1.3.3.5 Secure Connections to Servers

Administration when connecting to critical and sensitive systems should use SSH to authenticate and disable telnet and rlogin.

1.3.3.6 Monitoring servers

Administrators are to regularly monitor for invalid open network ports (using programs such as Netstat), and lists of open files for running processes (using for instance Lsof).

1.3.3.7 Other security considerations

Servers should have accounts administered securely, password construct rules, root access secured, file system security, use a screen saver and follow appropriate recovery procedures in the case of system compromise (see below 1.3.6).

1.3.4 Securing Linux Servers

Linux Servers should be secured like UNIX servers at the University and requires assessment and planning. Particular attention should be given to;

1.3.4.1 Harden servers

Unnecessary services and unneeded access should be disabled.

1.3.4.2 Other security

Linux servers are to be secured for booting (such as password protect BIOS and boot only from hard drive), the kernel (such as enable process accounting, disable unused features), packages installed or minimum number installed, the core operating system (such as shadow password), and filesystem used.

1.3.5 Securing Mac OS X Servers

In addition to that outlined in Sec 1.2.1 Fundamental IT Security Steps, MacOS X Servers having a full UNIX architecture for the most part can be secured like other UNIX servers. In particular, maintain a known image (SOE), turn-off default auto-login, disable ftp, telnet, file sharing and web sharing and use a screen saver with lock out when unattended for 10 mins.

1.3.6 Steps for recovery for UNIX and NT from compromise

In the event of a Server Compromise steps should be followed to respond to a UNIX and or NT system compromise. These include consulting management, notifying others in the organization, regaining control (such as disconnect server from network), analysis of the intrusion and installing a clean version of the operating system before connecting back to the network. Recovery procedures can include detecting a compromise, recognizing trojan horses, identify back doors, document steps taken, and disconnecting the server from the network. Guides by AusCERT can be used;

<https://www.auscert.org.au/render.html?it=1974&cid=1920>

1.4 Viruses and Unwanted E-mail

1.4.1 Anti-Virus Packages for Windows and Macintosh

Ensure the latest McAfee Virus Scan software for PC and Virex for Macintosh is installed and it is set to automatically update. Note that if anti-virus software is in the middle of a virus scan this should not be cancelled. Guidance for students for configuration in the University setting can be found here;

<http://www.infodiv.unimelb.edu.au/compss/infosheets/virus.html>

1.4.2 Use Recommended E-mail Client

Many virus infections can be prevented by using the University's recommended E-mail client Eudora. Eudora does not have the same IT security vulnerabilities and common virus types affecting it as does Microsoft Outlook and Outlook Express. For further assistance in downloading and installing Eudora for Windows and Mac refer to the infosheets here;

<http://www.infodiv.unimelb.edu.au/compss/infosheets/email.html>

1.4.3 Anti-Spam Filtering

A centralised Anti-Spam (unwanted and unsolicited e-mail) solution for staff is available and allows staff to enable filtering and have some control over what is being filtered. General information and guidance can be found here;

<http://www.infodiv.unimelb.edu.au/systems/spam/>

Staff mail client configuration can be found here;

- Eudora (MAC and PC)

<http://www.infodiv.unimelb.edu.au/systems/spam/eudora.html>

- Outlook 2002 (PC)

<http://www.infodiv.unimelb.edu.au/systems/spam/outlook.html>

- Procmail (UNIX)

<http://www.infodiv.unimelb.edu.au/systems/spam/procmail.html>

- WebMail

<http://www.infodiv.unimelb.edu.au/systems/spam/webmail.html>

2 ASSET MANAGEMENT

2.1 IT Asset Register

An inventory of all IT assets assists in identifying, tracking and accounting in particular where an IT security is an issue. A sample asset register with some important components heading columns and sections below;

DEPARTMENT NAME:					
Completed by: YA		Existence (when last sited)	Location (incl. IP address)	Value	Assigned responsibility to
Physical asset ID #					
Web Server	128.3	Yes as of 10/6/03	Level 2 Rm203 128.250.128.3	\$15,000	Mr. John Smith (LANAD)
LAN Switch	128.10	No (At repair shop) 9/06/03	Secure Disposal 128.250.128.10	\$5,500	Mr. John Smith
Laptop	128.50	Yes 10/06/03	Level 2, Rm205 128.250.128.50	\$7,500	Dr. Jane Smithers
Software assets					
DB Filemaker Pro		Yes – last updated 10/06/03	WS1, L2, Rm203	\$1750	Mr. John Smith
Norton Internet Security (Mac)		Yes - last updated 1/06/03	L2, Rm203 128.50-128.100	\$95	Mr. John Smith
Outlook Express		Yes – last updated 5/05/03	WS3, L2, Rm203 128.250.128.101-200	-	Mr. John Smith
Data asset					
Research data set		Yes	WS3, L2, Rm205	\$17000	Dr. Jane Smithers
Database software		Yes	WS4, L2, Rm205	\$40,000	Dr. Jane Smithers

It may be possible to use [Themis](#) and other software to assist this, instead of the current recommendation for the Head of Department to maintain the list as a spreadsheet.

3 RISK ASSESSMENT

3.1 IT Risk Points

An IT Risk Review Process should include the points and possible model suggested below. The definitions used for likelihood, consequence, level of risk, controls and residual risk need to be considered for the area of IT under review, for instance for system availability, legal and liability issues.

Points to consider;

- The IT Risk Registers should broadly follow the [Australian Standards AS/NZS 4360:1999](#) (Risk Management) and the [University’s Risk Management Policy and Principles](#) (dated September 2002).
- It may be noted that what is a Risk and what is a Causal Event varies on perspective.
- The Registers include consideration of the broad categories of illegal behaviour by staff and students (where necessary seek legal advice).
- Summarize attempts to minimize the potential effects of risks and select those risks that are thought to be most important. Given sufficient resources, consideration of all risks could be documented.
- Update Risk Registers annually to reflect changes.

Tip: Consider your Residual Risk a work in progress and action plans should be drawn up according to the level of risk.

3.2 IT Risk Definitions

The meanings of terms used to describe Likelihood, Consequence, Level of Risk, Controls and Residual Risk are given below. The definitions are consistent with AS/NZS 4360.

- **Likelihood**

Used as a qualitative description of probability or frequency. The following table can be used as a guide for systems with back-up (built-in redundancy or failover), hence the likelihood reflects the failure of the system as a whole.

Likelihood	
<i>Rare</i>	Only occurs in exceptional circumstances
<i>Unlikely</i>	Once in 10 years
<i>Moderate</i>	Once in 3 years
<i>Likely</i>	Once per year
<i>Almost certain</i>	Expected; possibly more than once per month

- **Consequence**

The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event. The following table represents the maximum impact of a casual event (such as a hacker attack, denial of service).

Consequence	
<i>Insignificant</i>	Local effect only for < 1 hour
<i>Minor</i>	Interruption in major service < 1 minute, then full recovery; or local service < 1 day
<i>Moderate</i>	Interruption in major University function down > 2 hours on a working day, then full recovery
<i>Major</i>	Interruption in major University function > 1 working day, then incomplete recovery; local service > 1 week
<i>Catastrophic</i>	Complete failure of a major University function > 2 weeks

- **Level of Risk**

The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood. The level of risk can be derived from the table below;

Likelihood	Consequence				
	<i>Insignificant</i>	<i>Minor</i>	<i>Moderate</i>	<i>Major</i>	<i>Catastrophic</i>
<i>Rare</i>	Low	Low	Medium	High	High
<i>Unlikely</i>	Low	Low	Medium	High	Extreme
<i>Moderate</i>	Low	Medium	High	Extreme	Extreme
<i>Likely</i>	Medium	High	High	Extreme	Extreme
<i>Almost certain</i>	High	High	Extreme	Extreme	Extreme

- **Controls**

That part of risk management that involves the implementation of policies, standards, procedures and physical changes to eliminate or minimize adverse risks. Controls can relate to the existence of backups, disaster recovery plans, business continuity plans, and policies that are in place to address the particular risk.

Level of Control	
<i>Poor</i>	No effective controls in operation
<i>Fair</i>	Controls address risk only partly
<i>Good</i>	Controls address known risks and are in operation but are not fully documented and audited
<i>Excellent</i>	Controls in operation fully address known risks and have been externally audited and documented

- **Residual Risk**

The remaining level of risk after risk treatment measures have been taken.

Controls	Level of Risk			
	<i>Low</i>	<i>Medium</i>	<i>High</i>	<i>Extreme</i>
<i>Poor</i>	Medium	High	Extreme	Extreme
<i>Fair</i>	Low	Medium	High	Extreme
<i>Good</i>	Low	Medium	Medium	High
<i>Excellent</i>	Low	Low	Medium	High

3.3 Risk Register Sample

The table below is a sample register of IT risks.

No.	Risk	Cause	Likelihood	Consequence	Level of Risk	Controls	Residual Risk	\$	Insurance Gaps
1	Unauthorised download of Copyrighted material by student or staff.g. MP3	Poor policy knowledge, poor access control, poor computer configuration, staff/student not recognising or identifying important developments	High	Major – Copyright owners enforce rights, legal costs, reputation loss	Extreme	Fair – University Copyright Policy, Copyright Officer appointed, Student labs note Copyright signs, Border Router Access Control	Extreme		
2									

4. BUSINESS CONTINUITY PLANNING

Business Continuity Planning should be reviewed annually, where disaster recovery documents and plans are written for critical areas that flow from the risk register.

4.1 Back-Up Guidelines

It is important to do regular backups at virtually every level of system administration so there is no catastrophic loss of valuable data. Even with the level of hardware reliability available, it can not be over-emphasized the importance of performing regular backups, and subsequent testing for restoration of saved data.

When administrators and users alike are faced with intruder break-ins or the possibility of sensitive data being stolen, a good back-up strategy is required. A combination of incremental and full backups is usually best.

Some of the backup procedures to follow are;

- Use at least two or more complete sets of media backups. If using tape, retire a set of tapes after 50 cycles of use because of media degradation.
- Once a week, schedule a time to test backups by restoring randomly selected files. Choose files of varied sizes and positions on the media to ensure that file size limitations or file boundary problems are not present in your existing backups.
- At least once a year carry out a complete system restoration on a separate machine, and examine its integrity. Knowing that the prescribed procedures work as intended.
- When using tape media, occasionally restore selected files using a different tape drive e.g. helical tape drives. Alignment or speed differences could make your drive unique, rendering your tapes useless if that particular tape drive fails.
- Keep backup media far away from the system being backed up. A local disaster, such as a small fire in one or two rooms, could mean complete loss of data by destroying both the system and backup. Do not store all the media in the same location.
- Label every tape following a backup.
- Do a complete backup on systems that are installed for the first time or have undergone a security cleanup. Day zero backups are valuable when it comes to restoring files following a break-in. If it can be determined where a security problem existed in an initial installation, perform the full restoration, fix the problem, and then backup the system again as your new day-zero backup version. This reduces the possibility of accidentally restoring old, insecure version of the file system in future.
- Destroy or mark as unsafe all backups taken after there has been a known or suspected break-in. Make a full backup immediately after the system has been cleaned.

4.2 IT Disaster Recovery Plans

IT Disaster Recovery Plans should include the following;

- Event Log
- Recovery Plan
- Restoration Procedures

- Contact Details of key staff and contractors
- Inventories
- Testing and Review Schedules for the Plan

4.2.1 Event Log

A sample Event Log is appended below;

Date	Time	Entry by	Step	Action Taken

4.2.2 Recovery Plan

A recovery plan involves;

- Executive management to identify likely causes of disaster, its extent and estimation of downtime.
- Notification of key staff and contractors involved in recovery procedure
- Preparation of Event Log and documentation of process taken
- Notification of higher level executive where appropriate
- Communication to users and staff of identified problem and estimated duration e.g. e-mail, fax, web or telephone
- IT Help Line notified if appropriate

4.2.3 Restoration Procedures

Following restoration procedures;

- Review the Event Log and notify those advised of the problem that services have been returned to normal
- Ensure all software and/or consumables used from the Inventories section is returned to its original location
- Send a copy of the Event Log to appropriate management and executive for records.

4.2.4 Contact Details

Contact details for key staff should be noted and include both fixed line and mobile telephone numbers. Contact details should lists executive management, other University management, key staff, contractors, service providers and other backup contacts.

4.2.5 Inventories

The disaster recovery plan should include the location of off-site copies and backups for software, hardware, data, configuration information, details of maps and plans.

4.2.6 Testing and Review

The plan should be tested annually by testing all of the entries in the contacts list to ensure they are current and by inspection of the Inventories.

Each year the plan should be reviewed by the executive manager and comments made as to the updates.

A check with the Risk Management Office as to the appropriate insurance cover should also be made.

3.4 STAFF

Staff are responsible for:

- (1) Ensuring any computer systems that are assigned for their use are kept secure. This requires particular vigilance for computer systems taken off campus.
- (2) Ensuring computer systems assigned for their use have up-to-date anti-virus software active.
- (3) Reporting to their Head of Department or Dean, and the IT Security Coordinator in the Information Division, any perceived breaches of IT security at the University.

3.4a STAFF

Staff should familiarise themselves with IT Security procedures for personal computing. These should be practiced at all times.

These include:

- Complying with rules and regulations
- How to choose good passwords
- Exercising caution when handling executable files
- Physical security of the personal computer
- Maintenance of Anti Virus software
- Patching of operating systems and software (if applicable)
- Taking backups
- Reporting actual or suspected IT Security incidents

The following links provide information on personal IT Security:

- <http://www.infodiv.unimelb.edu.au/it-security/simstep.html>
- <http://www.unimelb.edu.au/Statutes/r81r7.html>
- <http://accounts.unimelb.edu.au/passwords.html>
- <http://www.cert.org/homeusers/HomeComputerSecurity/#6>

Staff should also ask their LITE for information on IT Security procedures specific to their working environment.

3.5 STUDENTS

Students are responsible for:

- (1) Using any computer available to them only for the purpose of pursuing their approved course of study.
- (2) Reporting any perceived breach of security to a member of staff.

3.5a STUDENTS

Students should abide by rules and regulations applicable to their use of University IT facilities.

In the case of a student using his/her private computer to connect to the University network, the student should undertake the responsibilities in points 1 and 2 of Section 3.4 of the IT Security Policy. Students should also practice good personal IT Security at all times. It is recommended that:

- a reputable and updated anti virus software be active on the computer
- the operating system and applications are regularly patched
- consideration for IT Security in the student's residential computing environment be given when accessing the Internet or connecting into the University network.

The University's Compliance Office has information on the proper use of IT:
<http://www.unimelb.edu.au/compliance/UCOguidelines/1.html>

3.6 INTERNAL AUDIT

Internal Audit will periodically undertake reviews to check compliance with this Policy.

4 BREACHES OF THESE POLICIES

Breaches of these policies may lead to disciplinary measures as determined by the Vice Principal (Information).

Note:

There are no IT Security Procedures written for this section of the IT Security Policy.

RELEVANT LINKS TO INFORMATION FOR THE UNIVERSITY

IT Security Policy:

<http://www.infodiv.unimelb.edu.au/it-security/docs/ITSecPol.pdf>

University Computing And Network (and Web) Facilities:

<http://www.unimelb.edu.au/Statutes/r81r7.html>

University Intellectual Property Policy:

<http://www.unimelb.edu.au/ExtRels/ASDiv/IPPolicy/>

Personnel Policy and Procedures - IT Matters:

<http://www.infodiv.unimelb.edu.au/it-security/pppsec.html>

Software Copyright - Roles and Responsibilities:

http://www.infodiv.unimelb.edu.au/SoftwCpyRightRoles4_1001.pdf