

The University of Melbourne

INFORMATION TECHNOLOGY SECURITY POLICY

1	INTRODUCTION	2
2	POLICIES	2
2.1	ASSET MANAGEMENT	2
2.2	EQUIPMENT SECURITY	2
2.2.1	<i>Secure Disposal</i>	2
2.2.2	<i>Removal of Property</i>	3
2.3	ACCESS CONTROL	3
2.3.1	<i>General</i>	3
2.3.2	<i>Location of Equipment</i>	3
2.3.3	<i>Cabling</i>	3
2.3.4	<i>Network Access</i>	3
2.3.5	<i>User Authentication</i>	4
2.4	ENCRYPTION	4
2.5	MONITORING.....	4
2.6	SYSTEM DEVELOPMENT AND MAINTENANCE.....	4
2.7	PERSONNEL	4
2.8	BACKUPS	5
2.9	WIRELESS NETWORKING.....	5
2.10	DIALIN ACCESS.....	5
2.11	RISK MANAGEMENT AND BUSINESS CONTINUITY PLANNING	5
3	RESPONSIBILITIES	5
3.1	INFORMATION STRATEGY COMMITTEE	5
3.2	VICE PRINCIPAL (INFORMATION), INFORMATION DIVISION AND THE IT SECURITY COORDINATOR	5
3.3	HEADS OF DEPARTMENT AND DEANS	6
3.4	STAFF	7
3.5	STUDENTS	7
3.6	INTERNAL AUDIT	7
4	BREACHES OF THESE POLICIES.....	7

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.

2.2 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.

2.2.2 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.

2.3 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.

2.3.2 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.

2.3.3 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>

2.3.4 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.

2.3.5 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.

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

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.

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.

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.

3.5 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.

3.6 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).