

University of New England

Information Technology Security Policy

Document data:

| | |
|--|-------------------------|
| Document type: | Policy |
| Administering entity: | ITD |
| Records management system number: | D11/30637 |
| Infrastructure Committee endorsement: | 27 July 2011 |
| Date approved: | 14 November 2011 |
| Approved by: | Council |
| Indicative time for review: | 3 years |
| Responsibility for review: | ITD Management |

Related policies or other documents: UNE Risk Management Policy, Rules for the Use of Information and Communications Facilities and Services, Audit Vulnerability Scan Policy, IT Security Objectives and Framework, General Password Policy, P2P File Sharing Policy, Personal Mobile Computing Policy, Standards and Guidelines for all Users of University Computing and Network Facilities, Standards and Guidelines for Desktop Computers, Standards and Guidelines for Non-Strategic Systems, Standards and Guidelines for Strategic Systems

1. Rationale and Scope

The University of New England (UNE) acknowledges an obligation to ensure appropriate security for all Information Technology (IT) data, equipment, and processes in its domain of ownership and control. This obligation is shared, to varying degrees, by every member of the university.

UNE's IT resources are a valuable University asset and must be managed accordingly to ensure their integrity, security and availability for lawful educational purposes. This document is intended as a high-level security policy statement for use by all University staff, students and users of the University's information technology resources.

The purpose of this policy is to ensure:

- The provision of reliable and uninterrupted IT services;
- The integrity and validity of data;
- An ability to recover effectively and efficiently from disruption; and
- The protection of all the University's IT assets including data, software and hardware.

This document will:

- Enumerate the elements that constitute IT security;
- Explain the need for IT security;
- Specify the various categories of IT data, equipment, and processes subject to this policy;
- Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the university may function;
- Indicate appropriate levels of security through standards and guidelines; and
- Outline the scope of IT Security.

2. Principles

2.1. Definitions

Security can be defined as "the state of being free from unacceptable risk".

The potential causes of these losses are termed "threats". These threats may be human or non-human, natural, accidental, or deliberate. The risk concerns the following categories of losses:

1. Confidentiality of Information.
2. Integrity of data.
3. Assets.
4. Efficient and appropriate use.
5. System availability.

These are defined as:

1. *Confidentiality of information* refers to the privacy of personal or corporate information. This includes issues of copyright.
2. *Integrity of data* refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.
3. The assets that must be protected include:
 - Computer and Peripheral Equipment.
 - Communications Equipment.
 - Computing and Communications Premises.
 - Power, Water, Environmental Control, and Communications utilities.
 - Supplies and Data Storage Media.

- System Computer Programs and Documentation.
Application Computer Programs and Documentation.
- 4. Efficient and Appropriate Use ensures that University IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.
- 5. Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

2.2. Domains of Security

This policy will deal with the following domains of security:

- Computer system security: CPU, Peripherals, Operating System. This includes data security.
- Physical security: The premises occupied by the IT personnel and equipment.
- Operational security: Environment control, power equipment, operational activities.
- Procedural security by IT, vendor, management personnel, as well as ordinary users.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

2.3. Reasons for IT Security

Confidentiality of information is mandated by common law, formal statute, explicit agreement, or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the University's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken huge resources to generate, and some of which can never be reproduced.

The use of University IT assets in other than in a manner and for the purpose for which they were intended represents a misallocation of valuable university resources, and possibly a danger to its reputation or a violation of the law.

Finally, proper functionality of IT systems is required for the efficient operation of the university. Some systems, such as the HR, Finance, Student Administration, and Library systems are of paramount importance to the mission of the university.

3. Policy

3.1. Roles and Responsibilities

3.1.1. Policy Management

Approval of the IT Security Policy is to be undertaken by the University of New England Council on the recommendation of the Vice-Chancellor.

3.1.2. Policy Implementation

Each member of the university will be responsible for meeting published IT standards of behaviour as outlined in the “Rules for the Use of Information & Communication Facilities & Services”.

IT security of each system will be the responsibility of its custodian.

Regular Risk Assessments on IT security will be done by custodians and reported as required to the Director – Audit and Risk.

3.1.3. Custodians

University information must be protected against unauthorised access, tampering, loss and destruction in a way that is consistent with applicable laws and also with respect to significance to University activities. In practice this information is segregated into logical collections of records and data held in IT systems and applications. To fulfil this objective, each collection of information must be associated with a ‘Custodian’ who is charged with the protection and management of the information held by the respective system.

- IT will be the custodian of all strategic system platforms.
- IT will be the custodian of the strategic communications systems.
- IT will be the custodian of all central computing laboratories.
- IT will be the custodian of all central audiovisual equipment.
- Directorates, Offices and Units will be custodians of strategic applications under their management control (e.g. Finance, HR, and Library).
- Faculties, Schools, Offices, or Units will be custodians of all non-strategic systems under their ownership.
- Individuals and IT will be custodians of desktop, mobile and personal computing systems under their control.

Custodians must assess and report on risks to IT security for systems or applications they are responsible for in accordance to UNE approved risk policy and procedures.

3.1.4. All Users

- Users must operate under the “Principles” and “Policy” in the “Rules for the Use of Information & Communication Facilities & Services”.
- Users must comply with the “Principles” and “Policy” in the “Rules for the Use of Information & Communication Facilities & Services” and other IT and general policies such as the “Code of Conduct for Staff” and “Communication Policy”.
- Users are responsible for the proper care and use of IT resources under their direct control.
- Users must use ‘Hard to guess’ passwords in accordance with the “General Password Policy”.
- Users are required to report any IT security breaches or risks to ITD management or UNE senior management.

3.1.5. University Services

It is recognized that various sections of the university provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these sections and IT in generation of standards and implementation of the policy. Some of these sections and their services are:

- Human Resources: Personnel selection, induction, and exit-processing.
- Registrar: Policies concerning information confidentiality/privacy.
- Campus Services: Physical building security.
- Library: Copyright and Intellectual Property.
- Finance: Financial transactions.

4. Procedures

4.1. Standards and Guidelines

Standards and guidelines related to this policy assist ordinary users and system custodians to meet their IT security responsibilities. These standards and guidelines are an integral part of this university’s IT Security Policy and therefore define it in detail.

These Standards and Guidelines will appear under the following classifications:

- Personal behaviour.
- Strategic systems.
- Computer.

- Communications.
- Desktop (personal) systems.
- School-based non-strategic systems.

4.2. Documents

This policy is enunciated by the following documents. The documents are split into two sections. Basic policies will apply to all users, where the advanced policies apply to specific groups within the University and may not apply to ordinary users.

Basic policies for all users (Staff & Students)

- IT Security Policy.
- General Password Policy
- Personal Mobile computing policy
- P2P file-sharing policy
- Standards and Guidelines for All Users of University Computing and Network Facilities
- Standards and Guidelines for Desktop Computers
- Audit Vulnerability Scan Policy

Advanced policies for custodians, system owners and application developers

- General Server Security Policy
- Change Management Policy
- Change Management Procedure
- Standards and Guidelines for Non-Strategic Systems
- Standards and Guidelines for Strategic Systems

4.3. Related policies and procedures

The following documents are related to this policy:

- UNE Code of Conduct for Staff.
- [AARNet Access & Acceptable Use Policy](#)
- [Communications Charging - Internet Services Procedure](#)
- [Communication Policy](#)
- [Disk Space Allocation Procedure](#)


- [Email List Policy](#)
- [Email Procedure](#)
- [Forum & Blog Procedure](#)
- [ITD Infrastructure Maintenance Window Procedure](#)
- [Information and Communications Infrastructure Policy](#)
- [Modem Charging Procedure](#)
- [Network Registration Procedure](#)
- [Rules for the Use of Information & Communication Facilities & Services](#)
- [Standard Operating Environment Policy](#)
- [Student Computer Laboratories Procedure](#)
- [Training Computer Laboratory Procedure](#)
- [User Registration Procedure](#)
- [Web Publishing, Content and Online Applications Policy](#)

5. Changes

The IT Security Policy is be a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

- Major changes will be made in consultation with Council, and with the approval of the Vice-Chancellor.
- Minor changes will be approved by the IT Director of the University.

Approval signature



The Hon Richard Torbay MP

Chancellor