



IT SECURITY POLICY

Date approved:	15 November 2005	Date Policy will take effect:	15 November 2005	Date of Next Review:	December 2010
Approved by:	Vice Chancellor				
Custodian title & e-mail address:	IT Security Officer scott_hamilton@uow.edu.au				
Author:	Scott Hamilton				
Responsible Faculty/ Division & Unit:	Information Technology Services				
Supporting documents, procedures & forms of this policy:	IT Intrusion Response Plan				
References & Legislation:	IT Acceptable Use Policy (including the Requirements Governing the Use of IT Facilities) Crimes Act, 1914 (Commonwealth) Student Conduct Rules				
Audience:	Public – accessible to anyone				
Expiry Date of Policy:	Not applicable				

Contents

1 Purpose of Policy.....	2
2 Definitions.....	2
3 Application & Scope.....	2
4 Policy Principles.....	3
5 Access and Acceptable Use	3
6 Policy Responsibilities.....	3
7 Administration and Implementation.....	5
8 Version Control and Change History.....	6



1 Purpose of Policy

1. This document sets out University policy on Information Technology (IT) Security.
2. IT security is concerned with ensuring the integrity and availability of information and services and due confidentiality of information. It is concerned with risk management and ensuring that controls are proportionate to risk.
3. The University recognises the importance of IT security. It is committed to ensure all business activities performed with the use of information technology are protected and maintained, and that sustainable procedures are in place to reflect “best practice” IT security.
4. The University recognises that successful implementation of IT security relies on having a well-informed user community combined with effective management procedures. This overarching IT Security Policy is supported by a comprehensive set of supplementary policies to ensure correct application of IT security. A structured framework for the reporting and handling of intrusions is in place as documented in the IT Intrusion Response Plan.
5. The University of Wollongong is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. The University’s IT Acceptable Use Policy defines the acceptable behaviour expected of users and intending users of the facilities. The University requires users to accept the IT policies and the Requirements Governing the Use of IT Facilities as a condition of their use. These are accessible on the University Policy Directory.

2 Definitions

Word/Term	Definition (with examples if required)
University	University of Wollongong
User	Any person using any of the University’s Information Technology Facilities
IT	Information Technology
IT facilities	Information Technology facilities operated by the University, whether owned or leased
IT system	A related set of hardware and software used for the communication, processing and storage of information, and the electronic form of the information that they hold or process. This definition includes, but is not limited to, computers and their peripherals and other communication equipment, communication networks and other telecommunication facilities used to link such equipment together, and the operating software used on all such equipment.
IT security	Information Technology Security
Chief Technology Officer	The Chief Technology Officer, Information Technology Services
ITS	Information Technology Services at the University of Wollongong
University Network	The network infrastructure used by the University of Wollongong including all network services on main campus, satellite campuses, and wholly owned subsidiaries with trusted access to UOW services

3 Application & Scope

1. This policy represents the University Institutional position and takes precedence over other relevant policies which may be developed at a local level.



2. All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Policy Principles

1. University IT systems will be protected by effective management of IT security risks at all levels of the University as laid down in the University's IT policies, guidelines and procedures.
2. The University's IT Systems will be provided, managed, and operated such that:
 - IT systems are protected according to criticality and requirements for confidentiality, integrity and availability.
 - Security measures are determined with regard to the costs and benefits. This includes consideration of the implementation, ongoing management and maintenance of security measures.
 - A minimum set of security controls are established that apply a base level of protection to all IT facilities including firewalls, network intrusion detection, network access control lists (ACLs), email virus scanning, desktop anti-virus, and network vulnerability scanning.
 - A structured intrusion response framework is established for the reporting and handling of intrusions to IT systems.
 - Responsibilities are assigned to key positions and roles with respect to the University's IT Intrusion Response Plan.
 - Regular monitoring programs are established to ensure the ongoing effectiveness of IT security measures including but not limited to network and systems vulnerability scanning, intrusion detection reporting, and network traffic reports.
 - Business continuity plans for critical IT Systems are developed and reviewed regularly.

5 Access and Acceptable Use

1. Users of the University IT facilities may be granted access to a range of IT facilities and may only use those facilities that they have been authorised to use.
2. The University requires users to accept the IT policies and the Requirements Governing the Use of IT Facilities as a condition of their use. These are accessible on the University Policy Directory.

6 Policy Responsibilities

1. The following responsibilities apply:

Chief Technology Officer

2. The Chief Technology Officer has the following responsibilities:
 - a. carriage of the University IT Security policies, guidelines and procedures;
 - b. determining the effectiveness of IT security measures through regular monitoring programs;
 - c. authorising the disconnection from the University Network of any IT system, or area in which it operates, that fails to comply with IT Security policies, guidelines and procedures.
 - d. reporting to the University Audit Management & Review Committee on security incidents and implementation of University Security Policy.

IT Security Officer

3. The IT Security Officer has the following responsibilities:
 - a. determining the effectiveness of IT security measures through regular monitoring programs;



- b. overseeing the effective use of security controls and recommending appropriate measures for the protection of IT systems;
- c. ensure the effective application of the IT Intrusion Response Plan;
- d. recommending to the Chief Technology Officer the disconnection from the University Network of any IT system, or area in which it operates, that fails to comply with IT Security policies, guidelines and procedures.
- e. authorising the disconnection from the University Network of any compromised IT system in accordance with the IT Intrusion Response Plan;
- f. communicating detected security exposures or known security exploits to the University community as appropriate.
- g. assisting with the operation of IT Security policies, processes and management framework. Propose improvements where shortcomings and gaps are identified.
- h. assisting with applying risk management practise to information security in order to properly protect information and to direct resources where required.

Deans, Directors and University Librarian, or business owners of IT Systems

4. Deans, Directors and University Librarian, or business owners of IT Systems have the following responsibilities:
 - a. appointing custodians for the security of the IT systems under their management;
 - b. ensuring that IT systems in their area of authority are operated and managed in accordance with University IT Security policies, guidelines and procedures;
 - c. ensuring security intrusions are dealt with in a co-ordinated and timely manner, and reported as outlined in the University's IT Intrusion Response Plan.

IT Support Officers

5. IT Support Officers have the following responsibilities:
 - a. developing, operating and managing the IT systems in their custody in accordance with University IT Security policies, guidelines and procedures;
 - b. maintaining IT security awareness of users of the IT systems in their custody;
 - c. periodically monitoring and reassessing their IT security measures to ensure their effectiveness and to respond to changes in requirements;
 - d. immediately reporting all security incidents and breaches to the ITS Security Officer as outlined in the University's IT Intrusion Response Plan;
 - e. responding to security directives issued by the ITS Security Officer consistent with the University IT Intrusion Response Plan; and
 - f. facilitating access, physical or otherwise, to an IT system in accordance with the University IT Intrusion Response Plan.

Individual Users

6. Individual users have responsibility to:
 - a. act in accordance with the University IT Security policies, guidelines and procedures at all times;
 - b. be aware of the security requirements of the IT systems they use, and take every precaution to safeguard their access to these systems against unauthorised use; and
 - c. immediately report any known or suspected security incidents and breaches to the local IT Support Officers or ITS Security Officer.



7 Administration and Implementation

IT Security Administration

1. The University makes provision for the administration of IT security through the relevant organisational area within ITS. This group performs functions involving:
 - a. provision of global security measures for the protection of IT systems;
 - b. establishment and education of standards;
 - c. identification of security threats and vulnerabilities;
 - d. administrative support and advice and provision of solutions; and
 - e. participation in security audits and evaluations including relevant advice to custodians of IT Systems within the University.
2. Cooperation and collaboration with business owners and IT support officers across the organisation is required to perform these tasks. The cooperation and collaboration with law enforcement authorities may also be required from time to time.
3. The University reserves the right to isolate an IT system, restrict access, and/or restrict usage of an IT system that they reasonably consider to be a threat to University IT facilities.

Monitoring

4. The University reserves the right to monitor IT systems and carry out detailed security audits of any systems and data. Access to any data will always be via network or systems administrators, or via persons nominated by the Chief Technology Officer.
5. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

Compliance

6. The University treats misuse of its IT facilities seriously. Violations of the conditions of use of IT facilities may result in temporary or indefinite withdrawal of access, disciplinary action under the University's, or relevant entities, discipline procedures, and/or reimbursement to the University.
7. IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Technology Officer or their nominee will be the Primary Investigation Officer of allegations of IT misconduct by students. Detailed investigation procedures and the penalties that may be awarded to students engaging in IT misconduct can be found in the Student Conduct Rules.
8. A user's access will be withdrawn given a written request from an appropriate staff member of the sponsoring organisation. Access may also be withdrawn by ITS in response to a suspected policy violation.
9. A student whose IT access has been withdrawn as a result of an investigation under the Student Conduct Rules can appeal the decision or the penalty to the Student Conduct Committee. Otherwise, a user whose access has been withdrawn may request reconsideration of the decision by the Chief Technology Officer who shall consider the withdrawal with the relevant Senior Executive, Dean or Director or the University Librarian. Following this the Chief Technology Officer shall confirm the withdrawal or reinstate access.
10. Misuse or unauthorised use of University IT facilities may constitute an offence under the Crimes Act, 1914 (Commonwealth) and/or other pieces of State or Commonwealth legislation. Nothing in this policy or the Requirements Governing the Use of IT Facilities may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.
11. Users are encouraged to report any misuse and any reports will be treated as confidential.



8 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	15 November 2005	Vice-Chancellor	Approved version following IT Forum Feedback including Additional points regarding risk management
2	6 May 2009	Vice-Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh
3	9 March 2010	Vice-Principal (Administration)	Future review date identified in accordance with Standard on UOW Policy