UTS Information Technology Security
Vice-Chancellor's Directive

Abstract

The UTS Information Technology Security Vice-Chancellor's Directive defines the fundamental principles for the protection of UTS information resources and the proper controls needed to ensure compliance with internal and external regulatory and legislative requirements and to uphold the University's reputation. All users who are provided access to UTS information technology resources are responsible for ensuring compliance with this Directive.

Dates	Directive approved Directive takes effect Directive is due for review (up to five years)	07/02/2014 28/02/2014 02/2019
Approved by	Vice-Chancellor	
Implementation Officer	Chief Information Officer	
Relevant to	All users of UTS Information Technology resources	
Related documents	Intellectual Property Policy Privacy and Protection of Personal Information Vice-Chancellor's Directive Research Ethics policies and guidelines (under review) IT Security Standards (PDF) IT Security Incident Reporting Procedure UTS Risk Management Guidelines	
Legislation	University of Technology Sydney Act 1989 (NSW) Crimes Act 1900 (NSW) Criminal Code Act 1995 (Cwlth) Privacy Act 1988 (Cwlth) Privacy Amendment (Enhancing Privacy Protection) Act 2012 Privacy and Personal Information Protection Act 1998 (NSW) Copyright Act 1968 (Cwlth) / Copyright Amendment Act 2006 (Cwlth) Evidence Act 1995 (NSW)	

	Office of the Australian Information Commissioner — Privacy guides Government Information (Public Access) Act 2009 (NSW) Electronic Transactions Act 1999 / Electronic Transactions Amendment Bill 2011 (Cwlth) Workplace Surveillance Act 2005 (NSW) Surveillance Devices Act 2007 (NSW) Telecommunications Act 1997 (Cwlth) Telecommunications (Interception and Access) Act 1987 (NSW) Crimes (Forensic Procedures) Act 2000 (NSW) Spam Act 2003 (Cwlth) ISO Standards: • ISO/IEC 27001:2005 Information security management systems • ISO/IEC 27002:2006 Code of practice for information security controls
File number	UR12/1005
Superseded documents	Information Technology Security Policy (2000)

Contents

1. Purpose

UTS is committed to ensuring appropriate security for all information technology data, equipment and processes within its domain of ownership and control.

This UTS Information Technology Security Vice-Chancellor's Directive aims to:

- secure the University's assets against theft, fraud, malicious or accidental damage, breach of privacy or confidence through the use of its information technology facilities, including any UTS systems hosted externally, and
- protect UTS from damage or liability arising from the misuse of its information technology facilities.

2. Scope

This Directive applies to users provided access to UTS information technology resources, UTS affiliates, subsidiaries, staff, third party consultants, contractors and vendors.

3. Definitions

Information owner refers to the person with assigned responsibility for the appropriate use and protection of the specified information, and who is responsible for establishing rules and procedures governing the generation, storage, processing, dissemination and disposal of that information.

Information technology security incident refers to a violation or imminent threat of violation of security policies or standard information security practices.

Information technology and communication resources refers to anything related to computing technology, such as networking, hardware, software, the internet; for example, the University's online presence or the people that work with the technologies owned or provided by UTS.

Resource administrator refers to the person(s) at UTS with technical responsibility for an IT system.

UTS affiliates include honorary appointees, emeritus professors, contractors, volunteers, agency staff, members of University/faculty committees and any other person appointed or engaged by UTS to perform work, duties or functions for UTS.

4. Directive principles

High-risk aspects of the operation of UTS information and communication resources will be managed by establishing appropriate, documented directives and standards so that security processes are consistent with the latest industry protocols and developments.

Information security processes and controls are developed considering any risks that impact business operations.

The following information security principles will apply to the security of UTS information technology systems:

- **Access control**: Access to UTS information systems is restricted to authorised users. Authorised users will be determined in accordance with an access control plan developed by the information owner.
- **Asset management**: The components of UTS information systems are inventoried, and information owners and resource administrators are assigned to ensure system security.
- **Compliance**: UTS information systems and related technologies will comply with all applicable legislative and regulatory requirements.
- **Human resources security**: Appropriate background checks will be conducted for staff in roles that involve elevated access to UTS information systems prior to employment.
- **Information security incident management**: All information security incidents will be reported and investigated in a timely manner, and recommendations acted on as appropriate.

- **Information systems acquisition, development and maintenance**: When acquiring, developing and maintaining new and existing information technology facilities and systems, UTS will identify, assess and mitigate security risks.
- **Physical and environmental security**: Information technology security risks related to the physical environment, such as access to individual computers, will be recorded in the Information Security Management System (ISMS) managed by the Information Technology Security Team.

5. Directive statements

5.1 Security standards and requirements

The UTS Information Security Management System is designed to define, control and manage information security activities and controls.

Security requirements are determined through a risk assessment and the resulting requirements are incorporated into a technology solution.

The UTS IT Security Standards (PDF) are based on the Information Technology – Code of Practice (ISO/IEC 27002:2006) for Information Security Management. This document assists users, information owners and resource administrators in meeting their information security responsibilities.

5.2 Establishing system security through risk assessment

Information owners will perform an initial and annual risk assessment for all information resources produced under their control, in accordance with the UTS Risk Management Guidelines.

The initial risk assessment will ensure that security controls implemented are adequate and appropriate for the articulated information protection requirements.

The University's Information Technology Security Team will maintain an inventory of risk assessments and their findings. Documentation of the risk assessment process assists in ensuring consistency and completeness, as well as accountability. Documentation of the analysis and results also provides a useful starting point for subsequent assessments.

5.3 Incident management

The UTS Information Security Team is responsible for implementation and management of the formal IT Security Incident Reporting Procedure.

Information technology security incident response procedures covering breaches of security and their subsequent impacts will be developed for each system, application or information technology solution used at UTS.

The procedures will be:

- comprehensively documented and regularly updated
- used to establish the cause of any security breach (accidental or deliberate) and report findings/ recommendations, and
- used to record corrective action taken and measures implemented to prevent recurrence.

The University's Information Technology Security Team will implement security controls or, where UTS Information Technology Division (ITD) does not have primary technical responsibility for a system, the resource administrator will monitor the

implementation and effectiveness of any corrective action, including any required changes to existing procedures.

All users of UTS information technology and communication resources must report any observed or suspected information technology security incidents as quickly as possible in accordance with that procedure.

UTS may refer any incident involving a possible breach of state, federal or international law to the appropriate authority for investigation.

5.4 Directive exemptions

Technical or business requirements may indicate the need for an exemption from this Directive for specific matters. Following an appropriate risk assessment, the Chief Information Officer or their delegate may authorise an exemption. Prior to submitting a request, the requestor should:

- document the control for which the exception is required, the reason for the exception and the risk introduced
- attempt to identify alternative controls that mitigate the risk due to the exception, and then
- obtain management approval from the faculty or unit requesting the exception.

All exemptions will be reviewed on a periodic basis.

6. Roles and responsibilities

Accountable Officer: Deputy Vice-Chancellor (Corporate Services)

Implementation Officer: Chief Information Officer

UTS Information Technology Security Team is responsible for:

- management, implementation and monitoring of the formal IT Security Incident Reporting Procedure and Information Technology Management System
- maintaining an inventory of IT-related risk assessments and their findings
- developing and maintaining standards and procedures and advising on implementation and breaches of these as required
- promulgating and communicating relevant standards, procedures and processes outlined in this Directive to all users as appropriate.

All users are required to comply with this directive and other documents referred to in it.

7. Version control and change history

Date	Version	Approved by (date)	Amendment
28/02/2014	1	Vice-Chancellor (07/02/2014)	New Directive, following rescission of Policy.