

Policy Title: **INFORMATION TECHNOLOGY**

Descriptors : 1) IT Governance 2) Information Systems 3) IT Access
4) Information Technology 5) IT Networks

Category : **Information Technology**

[Intent](#)

[Organisational Scope](#)

[Definitions](#)

[Policy Content](#)

[References](#)

[Contact Information](#)

1. **Intent**

To establish direction, procedures and requirements to maintain the confidentiality, integrity and availability of University information, communication and computing services.

2. **Organisational Scope**

This policy applies to all students, staff, Council or Council Committee members, contractors and visitors using information, communication infrastructure, computer systems and applications developed or installed within the University's information technology system.

3. **Definitions**

Access Control	A mechanism by which a system, process or person grants or revokes the right to access information, or perform an action
Application	Software that performs a specific task or function
Authentication	A process to verify the identity and permissions of an individual, such as a request to log-in to an information system.
Authorised Officer	A person to whom the Vice-Chancellor or where applicable the Chief Information Officer, has specifically assigned the authority to undertake the specific tasks on their behalf.
Backup	Making copies of information so that these additional copies may be used to restore the original after a loss of

	information
Broadcast Electronic Message	<p>A broadcast electronic message is any electronic message sent to:</p> <ul style="list-style-type: none"> • All staff/students (or a large subset of staff/students) of Edith Cowan University or • Is sent to staff/students outside of the area/department issuing the e-mail
Change Advisory Board	The body established under the Change and Configuration Management process to review and approve changes to production systems
Computing Facilities	Information systems designed to facilitate and enhance the academic programmes and business needs of the University
Configuration Item	Any component of an IT Infrastructure, including documentary items such as a Service Level Agreement, which is under the control of Configuration Management and therefore subject to formal Change Control.
Data Centre	A facility approved by the University to house information systems and associated components, such as telecommunications and storage systems
Electronic Messaging	Systems for the delivery of text or graphically formatted electronic messages
E-Mail	Electronic mail. E-mail is a store and forward method of composing, sending, storing, and receiving electronic messages
Encryption	The process of converting information into cipher or code in order to maintain confidentiality
Filtering	An information system designed to process an information stream and permit or deny access dependent on the content or address
Hardware	A physical computer system, peripheral or component
ICT	Information and Communications Technology
ICT Acceptance Criteria	Criteria set from time to time by the Chief Information Officer to ensure new systems or enhancements to existing systems meet the requirements of this policy and are suitable to operate on the University's infrastructure
Information System(s)	Any technology based information processing system
Internet	A worldwide, publicly accessible set of interconnected information systems
IT Service Desk	A single point of contact for all information technology

	incidents
ITSC	Information Technology Service Centre
ITSC Risk Register	A register of risks identified by ITSC, maintained in accordance with ECU Risk Management Guidelines
ITSC Security Guidelines	Guidelines maintained by ITSC to establish good practice for maintaining the integrity and security of the University's ICT environment
Laptop	A portable computer designed to function in the same manner as a standard desktop computer
Malicious Software	Any software intended to cause harm to or facilitate unauthorised access to an information system
Monitoring	The process of ensuring that a public electronic messaging system (such as a chat room or bulletin board) complies with relevant statutes, rules bylaws standards and policies, (generally prior to publication).
Network(s)	An interconnected set of Information Systems
Remote Access	Accessing Information Systems from a network external to the central University system(s)
Remote Access Service	A service provided to facilitate remote access
Risk	The chance of something happening that will have an impact on the achievement of the University's objectives. Risk is measured in terms of consequences and likelihood
Software	Applications and programmes designed to perform tasks on an Information System
University information	Information which may result in a loss of advantage or level of security if disclosed to others who might have low or unknown trustworthiness, such as financial information or student records.
Virtual Private Network (VPN)	A private communications network tunnelled through another network
Wireless Network(s):	Any network whose interconnections are implemented without the use of wires

4. Policy Content

SECTIONS

4.1 Information Technology Governance

- 4.2 Acceptable Use of Information Systems
- 4.3 Application and Information Systems Development
- 4.4 Electronic Messaging
- 4.5 Information Systems
- 4.6 Information Systems Access
- 4.7 Information Systems Hardware
- 4.8 Information Systems Protection
- 4.9 Information Technology Service Management
- 4.10 Internet
- 4.11 Network Access Control
- 4.12 Remote Access
- 4.13 Breaches

4.1 Information Technology Governance

4.1.1 Good Information Technology governance is the collective responsibility of ITSC, application owners and end users. It provides a coherent framework for ensuring the sustainability of the University's ICT environment in support of the University's strategic priorities.

4.1.2 The Chief Information Officer will be responsible for:

- Maintaining an appropriate governance structures for the implementation of the objectives identified in the five-year, annually rolling functional plan for information systems, technology and processes
- Maintaining and reporting on performance indicators demonstrating the performance of information systems and processes as identified by the Vice-Chancellor's Planning and Management Group (VCPMG);
- The implementation of the objectives identified in the five-year, annually rolling functional plan for information systems, technology and processes;
- A risk-register documenting known risks relating to information systems.

4.2 Acceptable use of Information Systems

4.2.1 Information systems are provided for the purpose of teaching, learning, research, engagement and sustaining the business of the University.

4.2.2 The use of information systems is subject to relevant University policies and conditions designed to maintain the confidentiality, integrity and availability of information, and to generate an academic and administrative environment that is:

- stable
- sustainable
- productive
- ethical
- legal

- secure
- facilitative
- effective.

4.2.3 Right to Examine

The University reserves the right to examine any information on its facilities and to monitor use. Such examination may only be authorised by the Vice-Chancellor or an officer authorised by the Vice-Chancellor, or the individual owner of the information, or may be pre-approved where required by law.

4.2.5 Privacy

Personal Information stored by the University may only be disclosed to internal or external parties in accordance with the University's Privacy Policy, or may be pre-approved where required by law.

4.2.6 Authorised Users

Persons authorised to use University information systems are:

- Students enrolled in the University
- Staff employed by the University
- Other persons authorised by the Vice-Chancellor or an officer authorised by the Vice-Chancellor.

4.2.7 Proof of Status

A current, personal, University identity card is proof of identity for use of computing facilities. A University identity card should be carried at all times when using on campus computing facilities.

Failure to produce a card when requested by security officers and/or University staff may result in being requested to leave the area.

4.2.8 After Hours Access

Many computing facilities are available outside of normal University business hours. An access card may be issued by Security to an individual, and is not transferable.

4.2.9 Authentication

No attempt should be made to avoid authentication.

4.2.10 Acceptable Use

Information systems may only be used for the purpose for which they have been provided and not for other purposes.

University information systems may only be used with prior authorisation as set out in 4.2.66 Authorised Users.

4.2.11 Personal Conduct in shared computing facilities

Campus computing facilities are work places. Users of the facilities must respect the equipment/facility and the needs of other users.

4.2.12 Information Security

Accounts to access University information systems are for the exclusive use of an authorised individual and must not be used by others. Every reasonable precaution should be taken to ensure that passwords, accounts and information are adequately secured.

4.2.13 Copyright

Individuals must take care that they do not breach copyright law in their use of information systems, for example by:

- Downloading copyright protected material from the Internet.
- Accessing, installing or executing copyright protected material which is not legally obtained.
- Attempting to duplicate copyright protected software provided for use on University information systems.

Penalties for breaching copyright laws are substantial and the end user may be liable for any such breach.

4.3 Application and Information Systems Development

4.3.1 Project Proposals, Requests for Tender and Project Plans should be assessed by the Chief Information Officer or person authorised by the Chief Information Officer to ensure that they are capable of meeting the standards and obligations stated within the ICT Acceptance Criteria.

4.3.2 Identified risks with new applications or information systems must be recorded in the ITSC Risk Register.

4.3.3 Development environments and information must be on logically or physically separate hardware from production systems. Modifications to production systems must first undergo formal testing within a development environment.

4.3.4 Any changes or modifications must follow the procedures outlined in section 4.9 (Information Technology Service Management) of this document.

4.3.5 Prior to a new information system being developed or acquired the sponsoring Centre/Faculty management of the system must specify relevant information security requirements. Alternatives must be reviewed with the developers and/or vendors so that an appropriate balance is struck between information technology security and University objectives.

4.3.6 Requirements for ensuring authenticity and protecting data integrity in applications must be documented, and appropriate controls identified and implemented.

4.4 Electronic Messaging

4.4.1 University electronic messaging systems are not intended for personal use. Reasonable private use is, however, permitted providing it is not associated with any illegal or discriminatory activity, does not

adversely affect other users and does not adversely affect the good reputation of the University.

- 4.4.2 Any expression of personal opinion must not be made in such a way as to appear to be representative of the University.
- 4.4.3 Electronic messaging systems may include a function to broadcast messages to all recipients within the system. Such functions may be used as a communication mechanism in one or more of the following circumstances:
- an emergency situation has arisen and the message would initiate or assist with an emergency response;
 - communications involving safety, security or urgent Information Technology matters must be disseminated; or
 - a major announcement of strategic concern to the University is required.
- 4.4.4 Broadcast messages must be approved by one of the following University staff:
- Vice-Chancellor
 - Deputy Vice-Chancellors
 - Vice-President Resources & CFO
 - Pro Vice-Chancellors
 - Executive Director (Governance & Planning)
 - Chief Information Officer or an officer authorised by the Chief Information Officer, (for information systems related matters)
 - Directors (for matters that fall directly in their portfolios)
 - Manager, Security Services (for security related matters).
- 4.4.5 Any system that provides a method of instant publication or feedback (such as blogs, wikis and bulletin boards) must have a written:
- **Acceptable Use Statement** – this statement should clearly explain the purpose and provide guidelines for the use of the system.
 - **Monitoring Statement** – this statement must document how messages are to be treated prior to publication, after publication and archival parameters (as information ages, etc). In particular, this statement and the method that it describes should provide reasonable assurance that publications will comply with the Acceptable Use Statement.

These statements must be published in the same location as the system and shall be approved by the Chief Information Officer or an officer authorised by the Chief Information Officer.

4.5 Information Systems

4.5.1 The Chief Information Officer, or an officer authorised by the Chief Information Officer, will manage:

- Information security responsibilities and ensure that end users and application owners are aware of their information security responsibilities.

4.5.2 The Chief Information Officer will take all reasonable steps to ensure:

- The privacy of individuals' information stored on information systems, as required under any applicable legislation and the University's Privacy Policy.
- 'Acceptable use of Information Systems' section of this policy (section 4.2) is maintained, outlining the responsibilities for individuals using University information systems and computing facilities.

4.5.3 The Chief Information Officer is responsible for maintaining:

- i. Contact with authorities for the investigation of and prosecution relating to information security breaches.
- ii. The ITSC Risk Register in accordance with ECU Risk Management Policies and Guidelines.
- iii. Contact with special interest groups to ensure the ongoing identification of localised threats and vulnerabilities.
- iv. A register of all information technology assets for the purpose of identification, audit and investigation.
- v. Appropriate access controls and authentication mechanisms to ensure information is only accessible by authorised individuals and systems.
- vi. The 'Information Systems Protection' section of this policy (section 4.8), outlining the controls required to protect University information systems.
- vii. The ITSC Security Guidelines covering good practice in the areas of:
 - a. Password management
 - b. Account management
 - c. Authentication systems
- viii. An appropriate information security awareness programme to ensure the ongoing education of information security responsibilities to all individuals with access to University information systems
- ix. Appropriate plans, procedures, documentation and arrangements to ensure the recoverability of information systems in the case of a disaster or major incident.

- x. The Information Systems Access section of this policy (section 4.6), outlining the responsibilities and requirements for the:
 - granting of access to University systems;
 - use of University systems; and
 - revoking of access to University systems.
- 4.5.4 University information must, where possible, be stored on centralised information systems. Information held on individual desktop computers or portable computers such as laptops is the responsibility of the computer custodian to backup and keep secure. Any information held on individual computers must be transferred to the central system as soon as practical.
- 4.5.5 Passwords must not be shared with any other individuals unless the password is intended to be used for group purposes.
- 4.5.6 Passwords must be managed following good-practice as defined in the ITSC Security Guidelines.
- 4.5.7 Under no circumstances are purchased application system software to be copied without the express permission of the Chief Information Officer or an officer authorised by the Chief Information Officer,
- 4.5.8 Prior to being released to third parties, all documentation that describes University system procedures, operations and processes must be reviewed by the Chief Information Officer or an authorised officer, to ensure confidential information or intellectual property is not being inadvertently disclosed.
- 4.5.9 Unless specifically authorised by the Chief Information Officer or an officer authorised by the Chief Information Officer, individuals must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information security policy.
- 4.5.10 The Chief Information Officer will ensure that:
 - i. Procedures are in place for the reporting and management of information security threats and vulnerabilities.
 - ii. Any updates or changes to Information Security or Information Technology Service Management related sections of this policy are communicated where appropriate throughout the University.

4.6 Information Systems Access

- 4.6.1 The University provides computing facilities and access to information systems to individuals for University purposes. Personal use, private consulting work, computer games and other non-University activities must be limited and not in breach of University policies, and for employees this should not be undertaken whilst on duty.
- 4.6.2 Access to any University information system will only be granted in the following circumstances:

- I. To individuals who have obtained a student number or a staff number, as appropriate, or
 - II. To individuals who have been granted temporary access approval as a Visitor or Guest. Such accounts may be created at the discretion of the Vice-Chancellor or an officer, authorised by the Vice-Chancellor and under conditions set by the Vice-Chancellor or an officer authorised by the Vice-Chancellor, Visitor accounts must only be issued once an application for an account has been approved by the Chief Information Officer or an officer authorised by the Chief Information Officer,. Applicants must sign the 'Acceptable Use of Information Systems' form prior to being granted access to University information systems or
 - III. To students and staff from other Australian Universities on a reciprocal basis as agreed by the University. Applicants must be current enrolled students or staff and provide adequate supporting documentation from their University justifying access. Such documentation should be provided by:
 - For students, the Registrar (or equivalent position) of the University in which the student is currently enrolled; or
 - For staff from other Australian Universities, an authorised officer, of the University in which the staff is currently employed.
- 4.6.3 Access by an individual person to any University computing facility will only be granted after the "Acceptable Use of Information Systems" Policy and the associated form has been signed or electronically acknowledged.
- 4.6.4 All employees and contractors will be given a level of access to those information systems, and computer facilities commensurate with their need in order to perform their job or complete contracted tasks. Any attempt to access other systems or components of systems beyond their authorised level without prior University permission is prohibited and may result in disciplinary action.
- 4.6.5 All employees and contractors are required to sign a Confidentiality Agreement. This must be signed initially upon commencement of their employment, or the contract, and must be renewed on an annual or as required basis.
- 4.6.6 Upon termination or expiration of employment, or the contractual arrangement, access to all information systems will be revoked in accordance with the requirements of the ITSC Security Guidelines. On commencement of a subsequent employment, or contractors' arrangement all access will be reviewed and updated or revoked where necessary, with access granted only to information systems required to fulfil the requirement of their new position, or contracted tasks.
- 4.6.7 Access to data centre areas is granted only to authorised staff with a clear need to access the facility. Only those authorised by the Chief

Information Officer or an officer authorised by the Chief Information Officer, are to be granted access to data centres. Contractors or authorised visitors to data centres must be escorted by an authorised Information Technology Service Centre staff member at all times.

- 4.6.8 After-hours access to computing facilities is only granted to those University staff and students who require access for a legitimate University purpose.
- 4.6.9 Individuals using University remote access systems must comply with the Remote Access section of this policy as amended from time to time.
- 4.6.10 Individuals using University electronic messaging systems must comply with the 'Electronic Messaging' section of this policy (section 4.12).
- 4.6.11 Individuals using University Internet access must comply with the Internet Use section of this policy (section 4.10).
- 4.6.12 All individuals' passwords must be changed from time to time as determined by the Chief Information Officer in accordance with section 4.5.6.
- 4.6.13 Violations of access provisions are considered *misconduct* that may result in disciplinary action as set out in section 4.13, Breaches.

4.7 Information Systems Hardware

- 4.7.1 All University owned computer and communications hardware devices are to be covered by either a warranty agreement or a maintenance plan approved by the Chief Information Officer. Any such warranty agreement or maintenance plan must be consistent with the University's Business Continuity and Disaster Recovery planning requirements.
- 4.7.2 Unless the end user is in transit, University Laptops / portable computers, desktop computers and monitors must be securely attached to a desk at all times.
- 4.7.3 The security and safe keeping of University Laptops / portable computers is the responsibility of the assigned custodian at all times.
- 4.7.4 External disk drives and other portable devices containing University information must be locked away when unattended.
- 4.7.5 Data centres must be locked at all times and access should be on a need basis only. Rooms and cupboards containing cabling and network devices must be locked at all times and access should be on a need basis only.
- 4.7.6 Computers must not be removed or replaced when the assigned custodian of that machine is not present, unless prior permission has been obtained to do so.

- 4.7.7 Prior to disposal all information required to be maintained under the Universities Record Management Policy must be backed up to a secure storage device. All information must then be removed from computer, external disk drives and other portable devices prior to disposal ensuring that all information is irrevocably erased.
- 4.7.8 Equipment or hardware normally stored within a computing facility must not be removed without prior authorisation.
- 4.7.9 The Director, Facilities and Services Centre must ensure fire detection/suppression, power conditioning, air conditioning, and other computing environment protection systems necessary to assure continued service for critical University information systems are provided and maintained.

4.8 Information Systems Protection

- 4.8.1 The Chief Information Officer, or an officer authorised by the Chief Information Officer, must ensure appropriate backup procedures are established for recovery purposes. These procedures must meet or exceed any requirements agreed between ITSC and the application owner as part of the "ICT Acceptance Criteria" used to transition applications from development into production.
- 4.8.2 Information stored on data centre systems must be backed up for recovery purposes. These procedures must meet or exceed any requirements agreed between ITSC and the application owner as part of the "ICT Acceptance Criteria" used to transition applications from development into production.
- 4.8.3 Information backed up for recovery purposes must not be solely stored on the campus from which it originates. Backup information must be stored off-site, preferably replicated to another campus.
- 4.8.4 To protect the University's information and ensure business continuity it is essential that the University has an effective software management system. The system must:
- Minimize the risk of malicious software throughout the University
 - Have a central management function
 - Enable automated configuration and transparently provide:
 - Automated updates of malicious software data files
 - Upgrading of system version(s)
 - Downloading of new updates when required
- 4.8.5 The Chief Information Officer, or an officer authorised by the Chief Information Officer, will ensure systems are provided and maintained to:
- Monitor errors, performance problems and any abnormal activity or pattern of events
 - Monitor the activity of systems administrators
 - Detect unauthorised activity
 - Ensure monitoring systems do not record passwords or other authentication information that may be used to escalate privileges.

- 4.8.6 To ensure the reliability of activity and event logs when monitoring and recording system information, all systems on the University networks must include a time field that corresponds with the correct Western Australian time at the time of the event. The time must be stored at a level of granularity appropriate to the information system.
- 4.8.7 All University information systems must use secure authentication methods to ensure the confidentiality of passwords, codes and keys.
- 4.8.8 Sessions established with information systems must have appropriate timeouts and security measures to ensure unattended systems cannot be accessed by unauthorised individuals.
- 4.8.9 Access to administrative tools and security control systems are restricted. Unauthorised access and breaches of this policy may result in disciplinary action.

4.9 Information Technology Service Management

- 4.9.1 ITSC will only accept new systems for production after they have met the ICT Acceptance Criteria set by the Chief Information Officer.
- 4.9.2 The Chief Information Officer, or an officer authorised by the Chief Information Officer, will ensure the IT Service Desk is available to function as a single point of contact for incidents and enquiries.
- 4.9.3 Procedures for the recording, categorisation, investigation and ongoing management of incidents will be established, maintained and monitored.
- 4.9.4 Process, procedures and measures to ensure the identification of underlying cause will be established, maintained and monitored for the purposes of problem management.
- 4.9.5 A knowledge base of known errors will be established, maintained and monitored, including any appropriate work-around information.
- 4.9.6 A centralised database of Configuration Items will be established, maintained and monitored to ensure an accurate view of all controlled assets.
- 4.9.7 Process, procedures and measures to effectively manage change to Configuration Items will be established, maintained and monitored.
- 4.9.8 A repository of standard changes will be developed to assist with the system change management process.
- 4.9.9 A Change Manager will be responsible for the management and communication of changes to Configuration Items.
- 4.9.10 The Chief Information Officer will ensure a Change Advisory Board is established and operated to ensure adequate visibility of change control.

- 4.9.11 Only changes approved by the Change Advisory Board are to be made to production systems. Such changes are to be made only by staff authorised by the Chief Information Officer.
- 4.9.12 Process, procedures and measures to control the distribution and implementation of new software and hardware releases will be established, maintained and monitored.
- 4.9.13 Appropriate environments for the building and testing of releases will be developed.
- 4.9.14 All releases must adhere to the system change management process.
- 4.9.15 A regular, scheduled period, during which IT services may be made unavailable either in total or in part, is to be established. The period is to be used for maintaining IT services. The timing and duration of the period to be set aside for this purpose is to be negotiated by the Chief Information Officer or an officer authorised by the Chief Information Officer, with the following stakeholders:
- Deputy Vice-Chancellors
 - Pro-Vice-Chancellors
 - Faculty Deans
 - Executive Director (Governance and Policy)
 - Directors and Heads of Centres
- 4.9.16 All software used on ECU computers must be purchased by the University prior to its installation on University computers. Where required, such software must be covered by a current license agreement that is capable of being produced to the University, law enforcement officers or agents of the vendor.
- 4.9.17 Each Faculty and Centre is responsible for maintaining software license information in a register provided by the IT Service Centre and ensuring that all software installed on hardware owned by their business unit is appropriately licensed for use.
- 4.9.18 The Chief Information Officer is responsible for maintaining a software license register for centrally purchased software.
- 4.9.19 ITSC and Risk Management and Audit Assurance will periodically audit software registers against installed software to provide assurances on software licensing to the Senior Leadership Team and to Council.

4.10 Internet

- 4.10.1 Individuals wishing to establish a connection to the Internet using University information systems must authenticate themselves at a filtering mechanism prior to gaining access. Security controls and other restrictive mechanisms may apply to University internet access. No attempts to circumvent such mechanisms may be made, and breaches may result in disciplinary action. An individual may request access to certain filtered sites for the purposes of teaching, learning,

research, engagement and administration, with the granting of such access being at the University's discretion.

4.10.2 Unless the prior approval of the Chief Information Officer has been obtained, individuals must not establish Internet or other external network connections that could allow access to University information systems and/or networks and University information

4.10.3 In order to manage the cost of internet use, certain restrictions and controls are required and may be implemented by the Chief Information Officer. Excessive use is discouraged and fees and charges may be levied to business units in which excessive use occurs.

4.11 Network Access Control

4.11.1 No attempt is to be made by users to avoid any filtering or security systems designed to protect University information systems. Breaches may result in disciplinary action.

4.11.2 University networks must be kept logically separate to ensure that the principle of least privilege is adhered to.

4.11.3 No external network connection is to be created within the University network without prior authority from the Chief Information Officer or officer authorised by the Chief Information Officer.

4.11.4 No server is to be connected to the University networks without the authority of the Chief Information Officer. Unauthorised servers detected on the University networks may be disconnected without warning.

4.11.5 University information must not be hosted on University information systems accessible from the Internet without prior permission of the Chief Information Officer or officer authorised by the Chief Information Officer. Any risks associated with this University information must be recorded within the risk register (as described in the Information Security section of this policy).

4.11.6 University information must not be transmitted over unsecure networks such as Wireless Networks and the internet without appropriate encryption to ensure confidentiality.

4.11.7 Servers hosting University Information Systems are to be provisioned in a network protected from user networks and the Internet by an appropriate network access control mechanism, unless authorised by the Chief Information Officer or an officer authorised by the Chief Information Officer.

4.11.8 Access to University Information Systems via the network access control mechanism mandated in 4.11.7 above must be approved by the Chief Information Officer or an office authorised by the Chief Information Officer.

4.12 Remote Access

4.12.1 The Chief Information Officer will ensure systems are provided to grant individuals remote access to information systems to support the University's teaching and learning, research, commercial activities, community engagement and administrative functions.

4.12.2 All University policies as amended from time to time relating to the use of information systems, including regulations on ethical and legal use of University hardware, apply whilst using a remote access service. The use of a particular item of software through a remote access service should be consistent with the license agreement for that software.

4.12.3 All individuals using University remote access services should be aware that information saved to information systems which are not a part of the University system may be lost. Individuals should perform regular backups to ensure the ongoing availability of such information.

4.13 Breaches

4.13.1 The University may be required to report or disclose breaches and individual actions and information to an appropriate law enforcement agency or other third parties.

4.13.2 Individuals should be aware the University may consider breaches of this policy or failure to adhere to its terms as an act of misconduct and disciplinary action may be taken.

4.13.3 Depending on the severity of the breach the University may determine that serious misconduct has occurred.

4.13.4 Disciplinary action may include but is not limited to:

- Counselling; and/or
- Actions as provided within this policy; and/or
- Actions as provided within employment contracts, employment agreements and associated University policies; and/or
- Actions as provided within University Statutes and rules; and /or
- Criminal charges or civil action; and/or
- Dismissal
- Notifications of misconduct being made to an appropriate law enforcement agency.

5. References

Policy Code:	it043	File No: SUB/2909
Policy Owner:	Chief Information Officer	
Approved by:	Vice-Chancellor	
Date Approved:	14 July 2009	
Revision Date:	July 2012	
Amendments:		
Related Policies/Documents:	ITSC Application Acceptance Criteria Policy ICT Standards Security & Guidelines	

6. Contact Information

Contact Person:	Chief Information Officer
Telephone:	6304 3737
Email address:	g.trinder@ecu.edu.au



ICT Security

Standards & Guidelines

Effective from January 2011

Preamble

This document contains information about standards and guidelines that have been adopted at Edith Cowan University (ECU) for the protection of its information assets. The aim of this document is to provide guidelines for the interpretation of University policy as it applies in this area. This document should be read in conjunction with the Information Technology Policy (IT043).

More information about University Policy is available at the Governance and Planning Services web page (<http://www.ecu.edu.au/GPPS/policies>).

1. Introduction

1.1 Environment

ECU is a large University with an appropriate large number and mix of managed workstations (including desktop, laptop, tablet and netbook computers), mobile phones and servers in the environment. ECU also provides services to the many unmanaged devices that are brought to campus each day by staff and students.

The environment is complicated, and needs to be flexible in order to support the teaching, learning, research and administration of ECU.

Information plays an important part within the University with many applications developed and put in place to make University life easier for staff and students alike. The confidentiality, integrity and availability of that information is of utmost importance and therefore information security is a critical success factor for the University.

1.2 Threats

The aim of any information security system is to protect the confidentiality and integrity of the information and to ensure that it is available to the correct people in a timely manner.

There are many threats to these three basic requirements. Examples are:

- » Fraud;
- » Espionage;
- » Vandalism;
- » Accident;
- » Natural Disaster;
- » Malicious Software; and
- » Hackers

These standards and guidelines are structured in order to minimise these threats to the extent possible and while maintaining a balance between availability and risk.

1.3 Scope

These standards and guidelines support a set of policies, processes and procedures applying to all students, staff, contractors and visitors using information, communications infrastructure, computer systems and application developed or installed with the University's information technology system.

1.4 Audience

This document has been written with a broad audience in mind: all persons that may have access to the information assets of the University. Where possible, simple language has been used, but in order to avoid confusion technical terms may have been used (these are defined in the back of this document).

2. Security Principles for Edith Cowan University

2.1 Overview

The following principles are to be considered with respect to Information Security

- » **Business Requirements** – the first objective of information security is to ensure that the business is able to operate effectively and in a resilient and secure manner.
- » **Defence in Depth** – security is to be considered and implemented at as many levels as possible; this ensures that vulnerabilities and workarounds do not exist where one layer of security may be compromised or fail in some other manner. There are six security functions that provide defence in depth. These being deter, avoid, protect, detect, react and recover.
- » **Good Practice and Standards**– information security shall be structured in such a way as to provide good practice and standards in keeping with the need to balance risk, cost, security and effective operations.
- » **Peer Review** – where possible peer review shall be used to ensure that controls are in place and have been adequately documented and tested.

Other principles may be implemented by the CIO from time to time in order to ensure that the IT Services Centre is able to deliver its obligations under the University strategic and operational plans.

3. Roles and Responsibilities

3.1 Overview

The University community has a role with respect to information security (students, staff, contractors, visitors and the general public). Each of these groups has a specific set of responsibilities, based upon the level of access that they have been granted and their relationship with the University.

Information is provided for use in specific ways and purposes; the privilege of access is based upon taking up certain responsibilities to ensure that it is secure and protected.

3.2 University Security Responsibilities

Security responsibilities include the following roles at ECU:

- » **Vice Chancellor** – has ultimate accountability for information security.
- » **Chief Information Officer** – has responsibility for the development and implementation of security such as assisting asset owners in assessing risk and defining security measures, advising on security issues, investigating suspected security incidents and coordinating with other security organisations.
- » **Information Asset Owner** – is accountable for the security of their information assets.
- » **IT Management** – has responsibility for development, implementation, management and maintenance of information systems security as agreed with information asset owners and in accordance with University Policies.
- » **Users** – must be aware of their responsibilities relating to information security, and be accountable for their actions.
- » **Auditor** – must be independent (either within or outside of the University) who conducts reviews to provide assurance that information security policy and processes are complied with.

3.3 University Service Areas

All information within the University is owned by a particular service area; each service area is accountable for the security of the information that they may provide. There are many ways that information can be released inadvertently; only some of these are by technical means. Information owners need to be aware of all threats to their information and ensure that these are all appropriately controlled to their satisfaction.

3.4 Information Technology Services Centre

The IT Services Centre has a critical role in protecting information that is stored or made available electronically. By the nature of the systems that are used staff may have extensive access to information; given this threat, specific controls need to be enforced within the Information Technology Services Centre in order to protect information. These controls are the responsibility of the IT Services Centre.

3.5 Risk Management

Information security risks shall be kept within two locations: the risk register of the IT Services Centre (for general risks) and the risk register of the Information Asset Owner (for specific risks).

The information asset owner is accountable for ensuring that all risks are documented and mitigated to an acceptable level.

3.6 Security of Third Party Access

The availability of information systems to third parties (individuals or organisations) will be controlled. In particular, access to production information systems shall be restricted.

Third parties may include:

- » Hardware, software and facilities staff of service providers located off-site;
- » On-site contractors for hardware, software and facilities maintenance and support;
- » Cleaning, catering, security guards and other outsourced support services;
- » Student placements;
- » Casual short-term appointments; and
- » Consultants.

The University shall ensure that controls consistent with these guidelines are included in all contracts.

4. User Education and Responsibilities

4.1 Overview

University information systems may only be used with prior authorisation. Information systems may only be used for the purpose that they have been provided and not for any other purpose (such as personal use, private commercial or private consulting work) unless specifically granted by the Vice-Chancellor or an officer, authorised by the Vice-Chancellor and under conditions set by the Vice-Chancellor. ECU reserves the right to withdraw or modify authorisation or access to information systems without notice.

4.2 Acceptance of Responsibilities

The Information Technology Policy (IT043) of ECU defines an Acceptable Use Policy. This policy must be agreed to by all persons that have been granted authentication rights to information systems. Agreement to this policy is mandatory in order to be granted access.

4.3 Authentication

Authentication is an identity and permissions check performed with a user-id and password when a user logs on to a information system. No attempt should be made to avoid authentication.

Accounts to access information systems are for the exclusive use of an authorised individual and must not be used by others. Every reasonable precaution is to be taken to ensure that passwords, accounts and data are adequately secured. No attempt should be made to discover a password or gain access to another individuals account or information.

4.4 Unattended Equipment

Equipment should not be left unattended unless:

- » The equipment is secured from physical theft (cabled down, or within a filing cabinet or other secure, lockable location); and
- » The workstation has been closed down completely or a screen saver with a password has been activated.

In the event of equipment being left unattended it may be confiscated, or locked down for security purposes.

4.5 Reporting of Breaches of Policy

Any observed or suspected security weakness in, or threats to, systems or services should be reported. Users should not attempt to prove that such weakness exists.

5. Physical and Environmental Security

5.1 Data Centre Security

Data centres shall be secured via Access Control (provided by the Facilities Services Centre). Access lists for these locations shall be managed by the Chief Information Officer or an officer, authorised by the Chief Information Officer and under conditions set by the Chief Information Officer. All servers shall be located in a Data Centre unless otherwise approved by the Chief Information Officer.

The locations shall also have capabilities in order to manage:

- » **Power** – uninterruptable power supply (UPS) and backup generator;
- » **Heat and Humidity** – measurement and air-conditioning systems;
- » **Fire** – detection and suppression systems;
- » **Access** – access control systems, video cameras and other physical security measures; and
- » **Liquid** – liquid detectors shall be installed where there is a risk of inundation.

5.2 Equipment Security

Media, workstations, laptops, printers, mobile phones and other devices that may contain University information shall be secured. Particular attention should be paid to mobile and small devices. If equipment is to be left unattended it must be either:

1. Secured to a large object (such as a workstation being cabled to a desk);
2. Locked inside secure storage (such as a filing cabinet); or
3. Locked inside a secure room (such as an office).

It should be noted that office space does have some weaknesses (in particular during cleaning times, etc). It is recommended that options (1) or (2) be taken up even if the room is considered relatively secure.

Loss of any equipment which may contain University information should be immediately reported to the IT Service Desk and/or Campus Security.

6. Account Management and Access Control

6.1 Overview

University information systems may only be used with prior authorisation. Information systems may be used for the purpose that they have been provided for and not for other purposes (such as personal use, private commercial or private consulting work) unless specifically granted by the Vice-Chancellor or nominee.

Authentication is an identity and permission check performed with a user-id and password (or via similar means) when a user logs on to an information system. No attempt should be made to avoid authentication.

6.2 Operating System Access Control

Granting access to configure an operating system (on a server, workstation, laptop or embedded device) increases the risk of misconfiguration or the presence of malicious software. This may result in loss of productivity, data loss, or other undesirable effects. Users with access to operating systems (in particular administrative privilege) shall therefore be limited to those that require access by virtue of their role.

Administrative privilege shall be considered a privilege on all devices and shall only be granted to users that require access by virtue of their role. In order for administrative privilege to be granted, a staff member or student requires the following:

- » A need for administrative privilege that cannot be met in another manner, with confirmation of that need being provided by their line manager; and
- » Confirmation from IT Services Centre staff that there is no alternative method of achieving the desired outcome and that the risk to the University is minimal.

6.3 Application Access Control

The following needs to be considered with respect to application access:

- » **Identity** – unless otherwise approved by the Chief Information Officer (CIO) the key source of identity information shall be the Identity and Access Management (IAM) system. This system shall have interfaces to the student management and HR systems, but those systems contain partial identity information only and should not be used directly as a sole source of identity.
- » **Authentication** – authentication shall be provided via the Identity and Access Management (IAM) system. This system shall store username, password, token, biometric and other information used to authenticate a user. Other systems should not hold authentication information unless otherwise approved by the Chief Information Officer (CIO).
- » **Permissions** – the application owner (or their delegate) is responsible for the granting of permissions to their information system or application; these permissions will specify particular identities that are to be granted access along with an appropriate level of authentication (for assurance purposes).

Application permission shall be regularly checked to ensure that permissions are appropriate. Any permission deemed inappropriate as a result of this review shall be revoked immediately. Such checks are the responsibility of the application owner, supported by the administrator of the Identity and Access Management (IAM) system.

6.4 Monitoring System Access and Use

Information Systems shall be monitored to ensure conformity to access policy and standards. In order to have effective monitoring and audit tools, it is essential that logging of potentially damaging events – including exceptions, violations and other security-related events be performed, monitored and kept for a recommended period of time. Where possible event logs should include user id's, dates, times and a location/node identifier.

All system clocks should be adjusted and automatically synchronised to the correct time to simplify event tracking between multiple systems.

All users shall be made aware that monitoring is taking place and the privacy policies, procedures and guidelines of the University which control the use of logged information.

6.5 Non-ECU and Personal Equipment

All personal and non-University managed equipment shall be treated as hostile. For this reason, networks to which non-ECU devices may be connected shall be logically separated from networks hosting University systems.

7. IT Infrastructure Management

7.1 Operational Procedures and Responsibilities

Procedures for the management and secure operation of all systems and networks will be documented, along with statements of responsibility. These responsibilities shall be clearly allocated to specific staff based upon their position.

7.2 Backup and Housekeeping

It is essential that all infrastructure devices have a documented backup and housekeeping plan. The plan shall include:

- » All details of the backup system that is in place (frequency, retention period, testing, monitoring, etc).
- » All details of regular housekeeping to be performed (cleaning, visual checks, log management, monitoring, etc).

Documentation shall be kept up-to-date in a central location.

7.3 Incident Management Procedures

Incident management procedures shall be maintained by the IT Services Centre. It is the responsibility of each staff member within the Centre to understand the procedures, and their role within the procedure.

7.4 Protection from Malicious Software

In order to protect critical infrastructure systems from malicious software, the following shall be enforced:

- » All servers shall (as a minimum) have anti-virus and anti-malware software installed.
- » Access to production servers shall be minimised (see section 8.5 *"Segregation of Development Facilities"*).

7.5 Network Security Controls

Network security controls are required in order to ensure that:

- » Server networks are adequately protected, while allowing access for application, database and systems administrators;
- » On-campus University networks, equipment and workstations are protected from the Internet and other networks which may be considered hostile (such as wireless networks); and
- » The University complies with the requirements of the Australian Academic and Research Network (AARNet) and appropriate legislation.

The following capabilities are incorporated into the ECU network:

- » **Internet Firewall** – providing delineation between the University networks and external 'hostile' networks.
- » **Server Firewall** – providing delineation between the University network and networks which contain servers and equipment holding University information systems.
- » **Virtual Private Network (VPN)** – provides a service that allows staff and students to connect remotely to the network as if they were on-campus, and allows them to elevate their privilege in order to talk to secure systems.
- » **Content Filtering** – content filtering is used to ensure that certain inappropriate traffic is blocked. ECU uses a third-party system, and blocks traffic based upon a limited number of categories. Specific information is available in Section 15 of this document.

7.6 Media Handling

All media that may contain data from an Information System shall be treated in the same manner, and with the same restrictions, as the information system. This includes hard drives, tapes (including backup tapes), USB thumb drives and any other media.

Media shall be disposed of in a secure manner as per the requirements of the State Records Act. Policies and information with regards to the sanitisation of hard drives and magnetic media is available from the State Records Office at <http://www.sro.wa.gov.au/src/policies.asp>.

7.7 Maintenance

All infrastructure systems shall be under a documented maintenance and support agreement (all components: hardware, firmware and software).

8. Information Systems and Applications

8.1 Security Requirements Analysis and Specification

At the time of procurement security requirements should be specifically included in discussions. During preparation of tender documents, the following information should be included (customised as appropriate):

http://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

8.2 Security in Application Systems

Security requirements and controls should be established to reflect the value, importance or confidentiality of the information contained within an application, and the potential damage which may result from a failure or absence of security. Areas which may be considered include:

- » Segregation of duties;
- » Access controls for information systems files and functions;
- » Validation of input data;
- » Creation and regular review of audit trails for important events and attempted unauthorised access;
- » Procedures, documentation and training to allow the system to be used securely by non-specialist staff;
- » Creation and storage of backup copies of data and system;
- » Recovery from failures, especially for high availability applications;
- » Use of data encryption to protect data from unauthorised access, either during transmission or storage;
- » Use of formal change controls to ensure testing and authorisation of updates;
- » Use of version controls for IT system software and documentation;
- » Protection of test data, by ensuring any production data is 'de-identified' before use and removed after testing; and
- » Restriction on access to system audit tools, to prevent misuse or compromise.

8.3 Cryptographic Controls

It is important that sensitive data is encrypted when being carried over a network. As a minimum, strong cryptography shall be used where transmitting private or sensitive information (particularly authentication information) over any network.

Under all circumstances, encryption is preferred. Where present, the encryption implementation shall not result in any error messages or warnings. It is important that all encryption keys are correctly signed and distributed within the SOE, and made available to students via the main ECU website.

Cryptographic private keys shall be securely stored by the relevant ITSC technical staff.

8.4 System Acceptance

The IT Services Centre shall maintain a document named *Production Acceptance Guidelines* containing criteria set from time to time by the Chief Information Officer to ensure new systems or enhancements to existing systems meet the requirements of the Information Technology Policy and these guidelines.

8.5 Separation of Development Facilities

Equipment used for development ('DEV') and quality assurance ('QA') shall be separated from production ('PROD') systems. Passwords, cryptographic controls and access lists shall be separately maintained in order to ensure that access to production systems is limited as much as possible (while maintaining a level of redundancy and succession planning).

9. Business Continuity Management

9.1 Overview

Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.

Risk Management and Audit Assurance (RMAA) supports and audits the Business Continuity process at ECU. Each Faculty and Centre has the responsibility for ensuring the development, communication and ongoing support of the BCP associated with their areas of responsibility.

9.2 Business Continuity and Impact Analysis

A Business Impact Assessment (BIA) is a key process in measuring the level of impact to organisational activities, and is to be completed or reviewed annually, or following significant change in organisational structure or operational capability.

9.3 Business Continuity Planning Framework

Information about the Business Continuity Framework at ECU may be obtained from RMAA.

9.4 Testing, Maintaining and Reassessing Continuity Plans

Testing the effectiveness of the BCP within Faculties and Centres is to be undertaken at least annually and is to be supported by RMAA. Testing of BCP's may be undertaken as either of the following:

- » **Hypothetical** – Theoretical exercise;
- » **Component** – Exercising individual BCP components;
- » **Module** – Exercising a combination of the BCP components; or
- » **Full** – Exercising all BCP components.

Testing of BCP's is to be monitored by the Incident Management Advisory Committee and managed and coordinated by the respective Business Recovery Team and the Business Continuity Coordinator, RMAA.

10. Compliance with Legal Requirements

10.1 Compliance with Legal Requirements

All relevant contractual and statutory requirements will be explicitly defined and documented for each IT system, and the specific controls and responsibilities to meet these requirements will be defined and documented.

Proprietary software products are usually provided under a licence agreement, users of systems shall be aware of the limitations imposed by the licence agreement and comply with them at all times.

10.2 Review of Security and Technical Compliance

The IT Service Centre will adopt relevant standards for information security management and risk management, including WA Government Guidelines. Compliance with these guidelines is the responsibility of the Chief Information Officer, implemented by the ICT Threat Manager and other ICT staff as required. Compliance in this context means:

- » Regular reviews of security exposures;
- » Investigation of security infringements as required; and
- » An ongoing plan to achieve continuous improvement in security, within the operational budget allocation.

As a key guideline the University shall use Australian Standard 27001.

10.3 System Audit Considerations

The importance of independent audit as a control cannot be underestimated. It can take many forms, from reviewing other safeguards and identifying their strengths and weaknesses, to monitoring user behaviour and system activity. Audits are a key element in managing vulnerabilities.

When system audit tools are used, they shall be separated from the development and operational systems environments to prevent any misuse or compromise. Both software and data files should be restricted from access by IT personnel or users.

11. Definition of Terms

Authentication	A process to verify the identity and permissions of an individual, such as a request to log-in to an information system.
Authorised Officer	A person who has been specifically assigned the authority to undertake specific tasks on behalf of a more senior staff member.
Access Control	A mechanism by which a system, process or person grants or revokes the right to access information, or perform an action.
Application	Software that performs a specific task or function.
Backup	Making copies of information so that these additional copies may be used to restore the original after a loss of information.
Change Advisory Board	The body established under the Change and Configuration Management process to review and approve changes to production systems.
Computing Facilities	Information systems designed to facilitate and enhance the academic programmes and business needs of the University.
Configuration Item	Any component of an IT Infrastructure, including documentary items such as a Service Level Agreement, which is under the control of Configuration Management and therefore subject to formal Change Control.
Data Centre	A facility approved by the University to house information systems and associated components, such as telecommunications and storage systems.
Electronic Messaging	Systems for the delivery of text or graphically formatted electronic messages.
E-Mail	Electronic mail. E-mail is a store and forward method of composing, sending, storing, and receiving electronic messages.
Encryption	The process of converting information into cipher or code in order to maintain confidentiality.
Filtering	An information system designed to process an information stream and permit or deny access dependent on the content or address.
Hardware	A physical computer system, peripheral or component.
Information System(s)	Any technology based information processing system.
Internet	A worldwide, publicly accessible set of interconnected information systems.
ICT	Information and Communications Technology.
ICT Acceptance Criteria	Criteria set from time to time by the Chief Information Officer to ensure new systems or enhancements to existing systems meet

the requirements of this policy and are suitable to operate on the University's infrastructure.

ITSC	Information Technology Service Centre.
IT Service Desk	A single point of contact for all information technology incidents.
Laptop	A portable computer designed to function in the same manner as a standard desktop computer.
Malicious Software	Any software intended to cause harm to or facilitate unauthorised access to an information system.
Malware	See 'Malicious Software.'
Media Access Control (MAC) Address	A quasi-unique identifier attached to most computer network devices.
Monitoring	The process of ensuring that a public electronic messaging system (such as a chat room or bulletin board) complies with standards, policies, statutes, rules and bylaws (generally prior to publication).
Network(s)	An interconnected set of Information Systems.
Remote Access Service	A service provided to facilitate remote access.
Risk	The chance of something happening that will have an impact on the achievement of the University's objectives. Risk is measured in terms of consequences and likelihood.
Software	Applications and programmes designed to perform tasks on an Information System.
Virtual Private Network (VPN)	A private communications network tunnelled through another network.
Wireless Network(s)	Any network whose interconnections are implemented without the use of wires.

12. References

Code:	-	File No:
Owner:	Chief Information Officer	
Approved by:	Vice-President (Corporate)	
Date Approved:	-	
Revision Date:	April 2014	
Amendments:	-	
Related Policies/Documents:	Information Technology Policy (IT043)	

13. Contact Information

Contact Person:	ICT Threat Manager
Telephone:	+61 8 6304 6000
E-mail Address:	itservicedesk@ecu.edu.au

Appendices

14. Password Standard

The minimum password standard has been established based upon the following requirements:

- » It conforms to good practice of password selection;
- » It ensures that the minimum standards across all applications can be met; and
- » It enforces a character set that is supported by all applications.

For these reasons, the following structure is to be used:

Characteristic	Values	Description / Comments
Minimum password length	8 characters	8 characters is the good practice minimum for passwords;
Maximum password length	16 characters	16 characters is the maximum password length supported by Microsoft Live@edu.
Valid Characters	Numbers: 0-9 Letters: a-z, A-Z Punctuation: `~!@#\$%^&*()_+ = { } []\“” ; ‘<>? , . /	This is the base character set supported by Microsoft Live@edu and Oracle passwords.
First Character	The first character must be a letter or number (a-z or A-Z).	This is a requirement for Oracle database passwords.
Excludes	The password must not contain the username or the answer to the secret question. ¹	Good practice; required by Microsoft Live@edu.
Minimum Change Frequency	90 days	Good practice as supported by the Office of the Auditor General.
Password History	8 passwords	The password must not have been used in any of the past 8 changes.

¹ The Microsoft Live@edu service requires a secret question to be recorded in case a password is forgotten; this secret question is stored by Microsoft with a requirement that the secret question not form part of the password.

Appendices

15. Content Category Definitions

The classification of content is performed by the vendor providing the equipment and associated services. The vendor is currently Content Keeper:

ContentKeeper Technologies
218 Northbourne Avenue
BRADDON ACT 2512
Australia
Phone: +61 2 6261 4950
Fax: +61 2 6257 9801
E-mail: info@contentkeeper.com
Internet: www.contentkeeper.com
ABN: 30 079 874 481

Content is split into 32 separate categories (one being 'uncategorised'). The standard configuration at ECU blocks content within three categories: Adult Content, Malicious and Government Blocking List. Definitions of these categories are given below:

Category 1: Adult Content	A website is categorised under the Adult Content category if its contents includes the description or depiction of erotic sexual acts or sexually orientated material such as pornography. Exceptions to this are web sites that contain information relating to sexuality or sexual health, which may be classified under the Health Sites category (21).	Some examples are: www.playboy.com www.worldsex.com www.whitehouse.com
Category 19: Malicious	A web site may be classified under the Malicious category if its content is capable of causing damage to a computer or computer environment, including the unauthorised consumption of network bandwidth.	An example URL: astalavista.box.sk
Category 25: Government Blocking List	This category is populated by URL's which contain content that is deemed to be illegal by the Australian Communications and Media Authority.	Some examples are: Child pornography sites Bestiality sites Rape sites

The full list of categories is available on the ICT Wiki Site (restricted access) at <https://wiki.it.ecu.edu.au/display/ictm/Content+Filtering>.