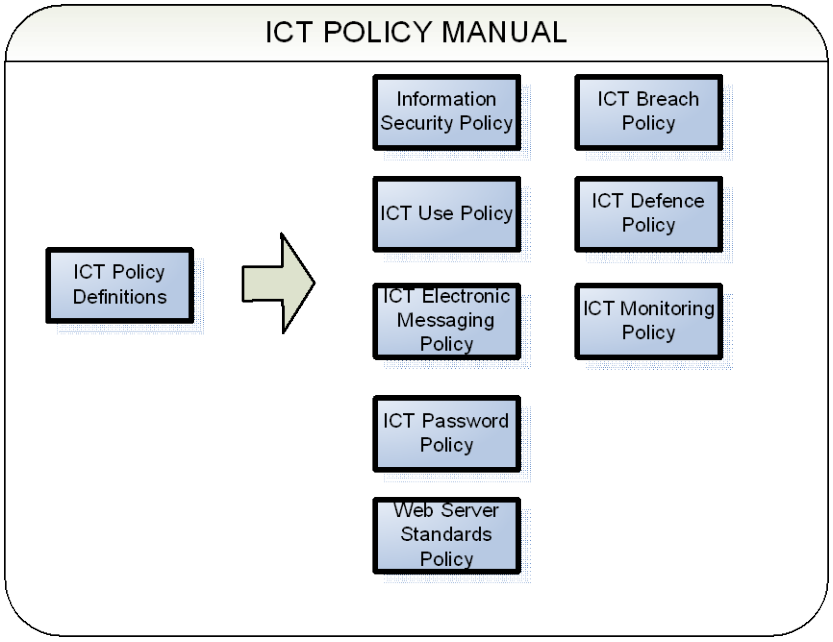
Curtin IT Services

ICT POLICY MANUAL

Version 4.0

Category: Information Management

CONTENTS



Information Security Policy

An amended version of this policy was approved at Planning and Management Committee on 28 July 2009, resolution PMC 79/09, Document No 01054/09.

This policy now exists in its own right and retitled in 2012 to *Physical and Information Security Policy*.

ICT Use Policy

PURPOSE

To ensure that the members of the University community may use University Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner and to ensure that other persons do not misuse those ICT facilities and services.

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

The University shall issue a unique username and password to staff, students, and University Associates to enable the appropriate and responsible use of Information, Communication and Technology (ICT) facilities and services.

Authorised users shall use University Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner. Incidental personal use of University facilities and services is permitted. Any other use is considered to be inappropriate use and action may be taken under the University ICT Breach Management Policy (refer to Schedule A - Appropriate Use of University ICT facilities and services for an overview of permitted uses).

Generic usernames (those that are not individually issued) shall only be issued under strict control procedures.

Access to these facilities and services is granted as a privilege; the University reserves the right to monitor, record and inspect electronic information and ICT-related activities; and to limit, restrict, cease, or extend access to Information and Communication Technology (ICT) facilities and services.

PROCEDURES

Usernames for Staff and University Associates
A username and password are automatically issued to each staff member and each University Associate as part of University business processes.

Usernames for Students
A username and password are automatically issued to each student as part of University business processes.

Compliance Education
The CIO shall provide examples of appropriate and inappropriate use of University ICT facilities and services. This information can be found in the Schedule to this policy.

OTHER RELEVANT DOCUMENTS/LINKS

Information Management Policy

Staff Confidentiality and Compliance Agreement

SCHEDULE A - Appropriate Use of University ICT facilities and services

A person using Curtin ICT facilities and services is responsible for ensuring that they comply with University ICT policies.

Appropriate use of Curtin ICT facilities and services includes but is not limited to:

(a) You shall use University ICT facilities and services in a manner which is ethical, lawful and not to the detriment of others.

(b) You shall use only those University ICT facilities and services you have been authorised to use.

(c) You shall only access ICT facilities and services on sites outside Curtin with the owner's permission and in a manner consistent with the owner's conditions of use.

(d) You shall actively defend your access to the University's ICT facilities and services from unauthorised use by others, including complying with the Password Policy (by keeping your password secret).

(e) When using University ICT facilities and services you shall produce your Curtin ID card if requested to do so by an authorised member of staff.

(f) You shall abide by instructions given by the Chief Information Officer or by their delegate. Such instructions may be issued by notice displayed in the vicinity of ICT facilities, by letter, by electronic communication, in person or otherwise.

(g) When you cease to be an enrolled student, a University Associate, or an employee of the University, your access to University ICT services and facilities will be terminated without notice. You are responsible for personal information you have stored on University ICT services and facilities and must make arrangements for its retention and/or removal as appropriate prior to leaving the University. Note that University records may only be disposed of in accordance with the *Information management Policy*.

(h) You may use University facilities and services for incidental personal use (e.g. occasional emails and web browsing during work breaks) provided that such use does not interfere with University business operations, does not breach any Federal legislation, State legislation or University policy or an ICT vendor's conditions of use or licence agreement. Some examples of interference with University business operations include: disrupting ICT facilities or services; burdening the University with significant costs; or impeding one's work or other obligations to the University.

What <u>not</u> to do…

(i) You shall not obstruct others in use of a Curtin ICT facility or service to achieve the functions and objectives of the University.

(j) You shall not use any account that has been created for another user without authorisation, nor shall you attempt to find out the password of another user, access or alter information, services, usernames, or passwords without authorisation.

(k) You shall not attempt to subvert security measures in any way, nor use a false identity when using ICT facilities and services.

(l) Without the explicit authorisation of the Chief Information Officer, you shall not possess any tools nor undertake any activities on Curtin ICT facilities or services that could result or assist in the violation of any Curtin policy, software licence or contract. Examples of these prohibited tools include viruses, Trojan horses, worms, password breakers, network packet observers or sniffers. Examples of prohibited activities include creating ping floods; spoofing packets; performing denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

(m) You shall not attempt to adversely interfere with the operation of any of the University's ICT facilities and services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, wilful interruption of normal operations, and accessing restricted areas without the permission of the Chief Information Officer.

(n) You shall not wilfully waste ICT resources. For example, wasting network bandwidth by downloading or sending large amounts of material that is neither work-related nor study-related.

(o) You shall not use the University's ICT facilities and services to send obscene, offensive, bogus, harassing or illegal messages.

(p) You shall not use the University's ICT facilities and services for commercial purposes nor publish or circulate information about other organisations via the University's ICT facilities and services, except where these activities clearly support the business or purpose of the University.

(q) You shall not use the University's ICT facilities and services in a way that breaches any University policy, such as the University Copyright policy.

(r) You shall not intentionally create, view, transmit, distribute, copy or store pornography or objectionable material via University ICT facilities and services unless it can be clearly demonstrated that it is required for teaching, learning, or research purposes.

(s) You shall not intentionally create, view, transmit, distribute, copy or store any information, data or material that violates Federal legislation or State legislation. For example, you shall not view, store, send, or give access to material regarded as objectionable by the WA Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40 (e.g. sexually explicit material involving children, incitement to violence, torture, and bestiality). You shall also not give a person under the age of eighteen years of age access to material regarded as restricted by the WA Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40 (e.g. matters of sex, drug misuse or addiction, crime, cruelty, and violence).

(t) You shall not attempt to conceal or erase the evidence of a breach of University ICT policy.

ICT Electronic Messaging Policy

PURPOSE

To ensure the University's electronic messaging services are used in an appropriate and responsible manner.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

The University permits users to use electronic messaging services in an appropriate and responsible manner.

A user's access to electronic messaging services shall be withdrawn:

- upon instruction by an Executive Manager, Head of School or Head of Area;
- when a staff member's employment with the University ceases;
- when a University Associate's association with the University ceases; or,
- when a student ceases to be eligible as a result of a change of enrolment status.

Records created by University staff during the course of University business are owned by the University and as such form part of Curtin's corporate assets. Users of electronic messaging services must be aware of their responsibilities in regard to the creation, capture, retention and disposal of University records (refer *Information Management Policy*).

Where access to University records is required in support of the University's business and purposes (such as files and email stored by a staff member who is on extended leave, or is no longer associated with Curtin), an Executive Manager may authorise CITS system administrators to grant another person access to that information. Please refer to the ICT Monitoring Policy for procedure to be followed.

PROCEDURES

Caveats in relation to Electronic Mail

Electronic mail is a public communication medium that uses a store-and-forward mechanism to pass each message through multiple servers owned by other organisations and via many communication links world-wide. It is subject to misuse by individuals and organisations worldwide, who send large numbers of unsolicited "spam" email messages to many email addresses.

As a result, the University cannot guarantee:

- The successful delivery of electronic messages travelling outside the University.
- The confidentiality of information contained in electronic messages travelling outside the University.
- That all "spam" email messages are blocked from entry to the University email system.

Limitation on Message and Attachment Size

Users shall minimise network traffic by reducing the size of large messages and attachments prior to transmission. Large files should be compressed before attaching them to the message to minimise network traffic.

Electronic documents in excess of any mail server's maximum allowable size may automatically be barred from transmission to the intended recipient. Large documents are best made available by sending recipients a link to the document; or in some cases, writing it to a CD or DVD and sending it by courier.

Appropriate Use of Electronic Messaging Services

Electronic messaging users shall act in a professional and ethical manner. For example, users shall:

- maintain professional courtesies and considerations in electronic communication.
- not transmit abusive or defamatory messages.
- not transmit an electronic message that breaches legislation (such as the *Spam Act 2003*) or contravenes University policies.
- not cause interference to other users of electronic messaging services. Examples of interference include transmission of e-mail chain letters, widespread distribution of unsolicited e-mail, junk mail, pyramid mail and the repeated sending of the same message.
- not give the impression that they are representing, giving opinion or making statements on behalf of the University, unless authorised to do so.

Non-compliance

Users who contravene this policy may be subject to the provisions of the ICT Breach Management Policy.

OTHER RELEVANT DOCUMENTS/LINKS

Information Management Policy

Staff Confidentiality and Compliance Agreement

SCHEDULE A Maximum permissible email message sizes

The Curtin staff Exchange email server will not send **or receive** any message which is greater than 20MB in size (including the message body and all attachments).

The Curtin student email server will not send any message which is greater than 5MB in size (including the message body and all attachments).

ICT Breach Management Policy

PURPOSE

To deal with inappropriate or irresponsible use of University Information and Communication Technology (ICT) facilities and services.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Each alleged breach shall be investigated to determine whether it was accidental or deliberate; this may determine whether any further action may be taken.

Users who are found to have breached a Curtin ICT policy shall be subject to disciplinary processes.

Management of a breach of policy is determined by the facts of matter. Penalties will be applied in line with University misconduct processes set out in the applicable employment instrument, contract of employment or University Statute and may include:

- Suspending the user's University network access.
- Suspending the user's University external Internet access.
- Recovering internet traffic costs associated with an Internet-related breach from the user.
- Censure or reprimand.
- Withdrawal of benefit.
- Dismissal

PROCEDURES

Incident Reporting

Information systems security incidents shall be reported to the Faculty ICT manager for assessment. The Faculty shall undertake a disciplinary process in consultation with People and Culture or Student Services (as appropriate) and the CIO or delegate, using the Schedules to this policy as a guide to the appropriate course of action.

Regardless of the level at which an incident is resolved, all information security incidents must be reported by the ICT support staff via Service Desk and assigned to the group **information security** to enable University-wide capture of incidents for reporting purposes. The identity of the alleged offender must not be identified in the service call.

Breaches of policy may be referred to the Crime and Corruption Commission, State or Federal Police upon the advice of the Standards and Integrity Officer and Legal and Compliance Services.

Breach Management Reporting

A quarterly management summary shall be provided to the Chief Information Officer. The names of persons who have breached ICT policy shall not be included in this report.

OTHER RELEVANT DOCUMENTS/LINKS

Information Management Policy

Staff Confidentiality and Compliance Agreement

ICT Defence Policy

PURPOSE

To defend Information and Communication Technology (ICT) facilities and services against attacks by computer malware.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Approved defensive measures shall be deployed and kept up-to-date on Information and Communication Technology (ICT) equipment, facilities and services owned or leased or provided by the University in Western Australia campus locations.

PROCEDURES

Faculty managers and system administrators shall ensure that desktop computers and infrastructure equipment in their area of responsibility complies with the defensive measures defined in the CITS Internal Procedures manual.

The Chief Information Officer may approve either exemption or part-compliance with this policy where the requirements of this policy cannot be fully implemented in a particular ICT facility or service for operational reasons. When exemptions or part-compliance with this policy are approved, the details of the approval will be forwarded to ICTC for noting.

OTHER RELEVANT DOCUMENTS/LINKS

NIL

Web Server Standards Policy

PURPOSE

The purpose of this policy is to minimise risks to the University that may arise as a result of incorrect information being made available through unauthorised Curtin web sites, and to ensure that Faculties, Schools and other organisational units have access to reliable web facilities and infrastructure.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

The Chief Information Officer may approve exemption or partial compliance with this policy where technical or operational reasons preclude full adherence.

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Material with Curtin URLs shall only be published on an Authorised web server. Authorised Web servers shall be managed to present a professional image of the University. Authorised web servers shall conform to CITS standards for server equipment, configuration and management.

Any material published electronically at Curtin that is found to be in breach of any Federal or State legislation, any Curtin Policy, or that significantly restricts or impacts on resources available to others may be removed without notice by authority of the Chief Information Officer.

International, Commonwealth, State and Local laws and the rules and statutes of the University shall take precedence over any policies contained within this document.

PROCEDURES

Registration and Approval

Except where approval has been granted by the Chief Information Officer or delegate, no web server shall be accessible via the World Wide Web beyond the Curtin communications network.

CITS shall maintain a register of Authorised web servers. Information contained in the register shall include web servers' physical and network addresses, and details of staff responsible for their maintenance. CITS may from time to time use information collected in the registration process to contact staff responsible for the maintenance of Authorised web servers.

Before material with a Curtin URL may be made accessible beyond the Curtin communications network, the web server on which the material is stored must be registered with CITS, and the configuration of the server must be compliant with the provisions of this policy. To request registration of a web server and thus enable it to publish material on the internet, the Web Server Registration form must be completed and provided to CITS.

Authorised web servers shall be managed to assure maximum availability for University clients. Down-time shall be scheduled with adherence to CITS change management procedures.

Web Server Management

Each Authorised web server must be managed by a designated officer who is part of a recognised ICT team to ensure appropriate levels of technical backup. The officer must be appropriately experienced to professionally manage the Authorised web server. Such officers must be authorised by their executive manager or delegate to act as the point of contact on matters related to the web server(s) in their charge.

The designated officer's name shall be registered with CITS as part of the web server registration process to ensure that contact may be made promptly as necessary.

Compliance

CITS shall from time to time survey Authorised web servers to determine:

- the hardware in use;
- the server operating system in use;
- the web server software in use;
- the latest systems patch installed;
- the latest server application patch installed.

Where any Authorised web server is found to be being managed in contravention of the provisions of this Policy and Procedures, steps may be taken to restrict access to it from beyond the Curtin communication network after reasonable consultation with the member of staff responsible.

OTHER RELEVANT DOCUMENTS/LINKS

NIL

ICT Monitoring Policy

PURPOSE

To ensure that the monitoring and inspection of information stored on University Information and Communication Technology (ICT) facilities and services is done in an appropriate and responsible manner.

APPLICATION

This policy is applicable to:

- All staff and students.
- All University Associates.
- All users of ICT equipment owned or leased by the University.
- All equipment connected to University data and voice networks.

EXCEPTIONS

DEFINITIONS

Refer to the document ICT Policy Definitions.

POLICY STATEMENT

Records created by University staff during the course of University business are owned by the University and as such form part of Curtin's corporate assets.

Electronic information stored on University ICT facilities and services may be subject to disclosure.

The University monitors electronic information and may inspect it, including electronic messages, in the following situations:

- Where it is required by law;
- Where it believes that violations of law or violations of University policy have taken place;
- To enable internal investigations into alleged misconduct to take place;
- To enable operational management of ICT facilities and services; and,
- To satisfy the requirements of the Freedom of Information Act 1992.

A staff member inspecting electronic information on behalf of the University is bound by the requirements of the Staff Confidentiality Agreement.

PROCEDURES

Authorisation to inspect electronic information

Inspection of electronic information shall occur only once it has been authorised in writing by any of the following:

- An Executive Manager;
- Director, Student Services;
- Director, People and Culture;
- The Chief Information Officer or delegate.

Where it is believed the circumstances may lead to investigation of potential breach of Curtin policy, the requester shall also consult with the Director, People and Culture or Director, Student Services (as appropriate).

Non-compliance

Any breach of this policy will be managed in accordance with the ICT Breach Management Policy.

OTHER RELEVANT DOCUMENTS/LINKS

Information Management Policy

Staff Confidentiality and Compliance Agreement

ICT Policy Definitions

The following definitions apply to all sections of the ICT Policy Manual:

Appropriate and responsible manner means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University Ethics and Social Justice Commitment Statement; it includes incidental personal use of University facilities and services.

Appropriate use means use that is consistent with the teaching, learning, research, University-based consultancy, and administrative objectives of the University and with the University's Values and Signature Behaviours; it includes incidental personal use of University facilities and services.

Authorised web server means a web server that is registered with Curtin IT Services and approved to publish material on the internet.

Breach means an information security incident that involves users not using Information and Communication Technology (ICT) facilities and services in an appropriate and responsible manner.

Business Owner means an authorised University officer or his/her delegate responsible for the management of a work area. A Business Owner authorises access to controlled ICT services.

Business or purpose of the University means an action or requirement which the University needs to have directly performed or met, in order to meet its objectives; or an action or requirement which will facilitate the achievement of the University's objectives.

CITS means Curtin Information Technology Services.

Controlled ICT service means an ICT service that only allows a user access after successful use of a username and password to authenticate themselves.

Copyrighted content means material for which the copyright for the content is held by a third-party other than the University, eg music, computer software, films, video.

Curtin communications network means that network of electronic communications equipment identified by Internet Protocol (IP) addresses within the ranges used by the University.

Curtin URL means a particular set of information on the Internet at a location with a Uniform Resource Locator that refers to a host either within the "curtin.edu.au" domain or within the IP address ranges used by Curtin.

Electronic Messaging Services means information technologies used to create, send, forward, receive, store, or print electronic messages.

Electronic Identity means the set of essential information about an individual that is stored electronically by the University.

Electronic Identifier means the value that is used in Curtin electronic systems to uniquely identify an individual. An electronic identifier is an attribute of the electronic identity.

Electronic Information means any information or recorded, either mechanically, magnetically, or electronically, within Curtin ICT facilities and services, including data, messages, music, computer software, films, video, etc.

Executive Manager means senior staff who have managerial responsibility for organisational area(s) within the University.

ICT means Information & Communication Technology.

ICTC means Information and Communication Technology Strategy Planning Committee.

Information and Communication Technology (ICT) facilities and services means any information resources provided by the University to assist or support teaching, learning, research and administrative activities. This includes, but is not limited to, physical spaces designated for teaching, study or research, all digital and electronic information storage, software and communication media devices, including, but not limited to, telephone, mobile phones, wireless or computer networks, computer workstation equipment including laptops, personal digital assistants, electronic email systems, internet, intranet and extranet. ICT facilities and services covers all types of ICT facilities owned or leased by the University, ICT services provided by the University and computer equipment owned or leased by users which are used to connect to the University networks and/or the Internet

Incidental personal use means infrequent and minor use of ICT facilities and services that does not: (a) interfere with University business operations; (b) breach any Federal legislation, State legislation or University policy; (c) breach an ICT vendor's conditions of use or licence agreement.

Information security incident means any information security event that disrupts the expected standard operation of ICT services and facilities.

Infrastructure means the physical equipment used to interconnect computers and users. Infrastructure includes the transmission media, including telephone lines, and also the router, aggregator, repeater, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals and data that are transmitted.

Malware means software written for malicious purposes such as computer viruses, worms, Trojan horses and spyware programs.

Objectionable material as defined by the Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40, includes material such as sexually explicit material involving children, incitement to violence, torture, and bestiality.

Operating System(s) means the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output.

Personal web server means equipment that normally functions as an individual person's desktop workstation that has been configured to publish material at a web URL.

Pornography means sexually explicit material that is not Objectionable material.

Qualified means having formal certification for administration of a relevant web server and its related operating system or evidence of successful completion of training courses and/or self-paced modules pertaining to the web server software and related operating system being used in a particular School or Area, or equivalent experience.

Record means any record, irrespective of format, created or received by an individual or group working on behalf of the University that relates to a business activity of the University and is kept as evidence of such activity.

Restricted material as defined by the Classification (Publications, Films and Computer Games) Enforcement Act 1996 No. 40, includes any material that a reasonable adult, by reason of the nature of the material, or the nature or extent of references in the material to matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, would regard as unsuitable for a minor to see, read or hear.

SEMS means Student Electronic Messaging Service.

Software means a specific use for a computer program, such as for accounts payable or payroll. The term is commonly used in place of the terms "application", "operating system" or "program." Examples of programs and software include pre-packaged productivity software (such as spreadsheets and word processors) and larger, customised packages designed for multiple users (such as e-mail).

Staff member means any person who has been offered and has accepted a contract of employment with Curtin University.

Student means a person who is admitted to, or enrolled in, a unit, course or program of study approved by Curtin University, which leads to, or is capable of leading to, an academic award of the University. For the purposes of this definition, the academic awards of the University are as recorded in the List of Academic Awards of Curtin University.

Student Electronic Messaging Service or *Student E-mail* means the electronic messaging services provided by the University to students via the University student portal.

University Associate means a person affiliated with and/or providing services to the University.

URL means Uniform Resource Locator, and defines the global address or location of a particular set of information on the World Wide Web.

University means Curtin University.

Use of Electronic Messaging Services means to create, send, forward, reply, copy, store, print, or possess electronic messages. For the purpose of this procedure, receipt of an electronic message is excluded from this definition to the extent that the recipient may not have control over the content of the message received.

User means a staff member, student or University Associate of Curtin University, and includes other persons given limited access to University ICT facilities and services in support of the teaching, learning, research, University-based consultancy, and administrative objectives of the University.

Virus means a particular type of software written for malicious purposes; viruses are part of the "malware" family.

Web server means a computer that publishes electronic information via either the http or https protocols.

World Wide Web means a system of Internet servers that support specially formatted documents. The documents are formatted to support links to other documents, as well as graphics, audio, and video files.

Policy Compliance Officer	Richard Addiscott, Director, IT Planning, Governance and Security
Policy Manager	Chief Operating Officer
Approval Authority	Planning and Management Committee
Review Date	1st April 2012

REVISION HISTORY:

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes and Notes
New	Approved	28/08/2007	PMC	PMC 75/07	Attachment to Document 00986/07 (Version 2, Revision 3)
	Amended	01/07/2008	PMC	PMC 58/08	Attachment A to Document No 00659/08
	Amended	02/06/2009	PMC	PMC 47/09	Name Change from Staff Services to Human Resources
	Administratively Amended	28/07/2009	Director, Legal and Compliance Services		Information Security Policy removed from ICT Policy Manual and exists in its own right (PMC 79/09, Document No 01054/09)
	Administratively Amended	27/07/2010	Director, Legal and Compliance Services		ICT Password Policy removed from ICT Policy Manual a new policy exists in its own right (PMC 66/10, Attachment A to Document No 00853/10)
	Administratively Updated	20/04/2015	Director, Legal and Compliance Services		Director, Human Resources changed to Director, people and Culture
	Administratively Updated	06/10/2015	Director, Legal and Compliance Services	EC 76/15	Executive Management Title Changes
	Administratively Updated	09/05/2016	Director, Legal and Compliance Services		Removal of Guiding Ethical Principles to Curtin Values
	Administratively Updated	09/02/2017	Director, Legal and Compliance Services		Area name change from Human Resources to People and Culture (also approved by the Chief Operating Officer)
	Administratively Updated	12/10/2017	Director, Legal and Compliance Services		Policy Compliance Officer updated