Information Security & Information & Communication Technology (ICT) Appropriate Use Policy

1. STRATEGIC PLAN THEME AND COMPLIANCE OBLIGATION SUPPORTED

Strategic Plan Theme: Sustainable Futures

2. PURPOSE

To ensure the University community is provided with a secure, and risk-appropriate information environment to enable Curtin to achieve its strategic objectives in an appropriate and responsible manner.

3. POLICY STATEMENT

3.1. Information Asset management security

3.1.1 All Information Assets will be identified and protected in a manner that is appropriate to their sensitivity and importance.

3.1.2 Information Assets will have an Information Asset Owner who is accountable for making decisions for the Information Asset's security.

3.1.3 Information Assets will have an Information Asset Administrator who is responsible for ensuring the overall controls applied to an information asset are commensurate with the information security classification and the risk profile of the information asset.

3.1.4 Information Assets will have appropriate protective controls applied throughout the asset's lifecycle that meet the Information Asset's security classification to include acquisition, development, maintenance, and decommisioning in accordance with organisational value, risk appetite, and legislative environment.

3.1.5 Information Assets will only be accessed, used and/or shared for the approved purpose of the Information Asset in accordance with supporting University policies and procedures (including the *Disclosure of Personal Information Procedures*). Any proposed changes to an Information Asset will consider the security of the asset.

3.1.6 Any security incidents affecting an Information Asset, such as where access to an Information Asset is unavailable, where the Asset been modified in an unauthorised manner, or where exposure of the Asset is contrary to its information security classification will be reported to the IT Security and Assurance team.

3.2. Appropriate use of ICT Assets

3.2.1 ICT Assets will be used for authorised purpose(s) only, such as official University business or University approved research and development, and limited Personal Use.

3.2.2 Users will act in a manner which complies with the University's values, relevant legislation, statutes, rules and applicable policies and procedures.

3.2.3 University staff will monitor, inspect and review the use of ICT Assets.

3.2.4 Users will not upload, download, install and or distribute unlicenced or inappropriately licensed software.

3.3. Password security

3.3.1 Information used to access Information Assets (such as passwords, personal identification numbers, passcodes and biometric information) will be protected. A User will not disclose University passwords to anyone, unless:

- the User (e.g. Information Asset Administrator) is issuing a new password; or
- the disclosure is approved by the Chief Information Officer, or their authorised representative.

3.3.2 All University ICT Assets will refer to the University ICT Password Security Standard.

3.4. Third party management

3.4.1 When forming contracts, Contract Owners will give due consideration to, and ensure provisions are made for all agreements with third parties to include the following, where relevant:

- appropriate information or data security provisions, including details relating to respective responsibilities for the security of Curtin's data throughout the course of the contractual agreement;
- provisions that enable Curtin to comply with its privacy expectations and legislative obligations;
- the right to audit third party and supporting Information Technology (IT) systems, services, processes and personnel activities and accesses;
- ensuring appropriately secure password security policies are applied to all ICT Assets, referring to the University ICT Password Security Standard;
- the return and deletion of Curtin data from the third party's IT environment; and
- a requirement to report security incidents, such as a potential loss or breach of information, exposure of information to an unauthorised third party, or a loss of availability of key services due to malicious activity to Curtin University.

3.4.2 During the course of a contract's life, the nominated Contract Manager will ensure the above provisions and associated responsibilities and performance measures are adhered to by all parties to the contract.

3.5. Information security risk appetite

The University has a low risk appetite for the unauthorised access, disclosure, modification and/or destruction of its Information Assets.

3.5 Responsibilities

3.5.1 These positions are responsible for implementation of the policy in their work areas:

- Executive Managers;
- Chief Information Officer;
- Contract Owners;
- Information Asset Owners;
- Information Asset Administrators; and
- Information Asset Users.

4. SCOPE OF POLICY

This policy applies to the University community in all Curtin University campuses, and where not already covered, to information assets owned, managed, controlled and leased by the University, or as applicable by commercial or legal arrangement.

5. DEFINITIONS

(Note: Commonly defined terms are located in the *Curtin Common Definitions*. Any defined terms below are specific to this document)

Chief Information Officer
As defined by University role, or in the alternative, the contracted Head of IT in offshore locations.

Contract Owner
Any authorised member of the University Community who awards a contract or who grants a deal for an assignment and takes the responsibility of paying the contractor.

ICT Assets
Any information, communications technology or audio-visual service, equipment or facility owned leased or contracted by the University that hosts, stores, transmits or presents digital information for the business and purpose of the University. This may include, but is not limited to:

- Software applications.
- Physical and virtual hardware.

- Email, messaging and collaboration applications.
- Any outsourced cloud or third-party services.
- Interconnected devices and embedded systems that can communicate or interact with other ICT Assets.
- Audio-visual systems and devices.
- Telephony, videoconferencing and web conferencing systems, services and applications.

Information Asset
Any knowledge or data (irrespective of format) that has value to the University and consequently needs to be suitably protected.

Information Asset Owner
An Information Asset Owner is a duly authorised representative of the University who is the nominated owner for one or more information assets by virtue of their position.

Information Asset Administrator
An Information Asset Administrator is a staff member or business unit (such as Digital and Technology Solutions (DTS)) of the University or otherwise contracted provider to the University who is responsible for the custody and security of Information Assets on behalf of the Information Asset Owner.

Information Asset User
Any member of the University Community who is duly authorised to use or access an Information Asset by the Information Asset Owner.

Information Security
Protection of the University's information assets from unauthorised access, disclosure, alteration, unavailability or detriment throughout the lifecycle of an asset.

Personal Use
Incidental use of ICT Assets that is not for the business or purpose of the University. For example, personal emails, online banking and social networking.

User
Those people or entities part of the University community that use University information or ICT Assets.

6. SUPPORTING PROCEDURES

Nil

7. RELATED DOCUMENTS/LINKS

External

- *Australian Privacy Principles* of the *Privacy Act 1988* (Cth) (also see Curtin's summary)
- *Copyright Act 1968* (Cth)
- *Criminal Code Act Compilation Act 1913* (WA)
- *Freedom of Information Act 1992* (WA)
- *State Records Act 2000 (WA)*

Internal

- *Code of Conduct*
- *Disclosure of Personal Information Procedures*
- *ICT Appropriate Use Procedures*
- ICT Password Security Standards
- *Information Security Classification Policy*
- *Information Management Policy*
- *Records and Information Management Procedures*
- Reporting Information Security Incidents
- Risk Management Framework
- *Risk Management Policy*

Policy Compliance Officer	Jeremy Iredell, Manager, IT Risk and Assurance
Policy Manager	Chief Operating Officer
Approval Authority	Senior Executive Team
Review Date	1st April 2024

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
New	Approved	18/09/2018	Planning and Management Committee	PMC 90/18	Attachment A to Item 8