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

1. COMPLIANCE OBLIGATION SUPPORTED

Cyber Security Act 2024 (Cth)
Security of Critical Infrastructure Act 2018 (Cth)
Western Australia's Cyber Security Policy

2. PURPOSE

To establish the University's cyber security risk management approach and appropriate use of ICT assets to ensure our University community is provided with a cyber-resilient and reliable digital experience.

3. POLICY STATEMENT

3.1. Cyber Security Risk Management

3.1.1. The University manages cyber security risks in alignment with its defined risk appetite.

3.1.2. Anyone in the University community who is responsible for ICT assets must regularly assess cyber security risks related to those assets.

3.1.3. The University will take all reasonable steps to continually improve its cyber security capabilities to govern, identify, protect, detect, respond to, and recover from cyber security threats and incidents.

3.2. Cyber-Aware Culture

3.2.1. The University will promote a strong security culture through education and awareness programs to improve cyber resilience.

3.3. Appropriate use of ICT Assets

3.3.1. ICT assets must only be used for authorised purposes, such as official University business, teaching, research. Limited incidental personal use is permitted as needed.

3.4. Responsibilities

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

a) Executive Managers;

b) Line Managers;

c) Chief Information Officer; and

d) Chief Information Security Officer.

4. SCOPE OF POLICY

This Policy applies to all members of the University community (which includes Council members, students, employees, University Associates, Curtin controlled entities, and all persons participating in University business or activities, including whether as a visitor, adjunct appointee, service provider, or contractor) in any location or campus within Australia and offshore.

5. DEFINITIONS

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

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 assets 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, networks, 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.

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

6. SUPPORTING PROCEDURES

Cyber Security Procedure
Information and Communication Technology (ICT) Appropriate Use Procedures

7. RELATED DOCUMENTS/LINKS

Internal

- Code of Conduct
- *Information Breach Policy* and *Procedures*
- *Information Management Policy* and *Procedures*
- *Privacy Policy* and *Procedures*
- *Risk Management Policy* and *Procedures*

External

- *Criminal Code Act Compilation Act 1913* (WA)
- *Freedom of Information Act 1992* (WA)
- *Privacy and Responsible Information Sharing Act (WA) 2024*
- *Privacy Act 1988* (Cth)
- Reporting Information Security Incidents
- *State Records Act 2000* (WA)
- *Higher Education Standards Framework (HESF): Standards 2.1.2 & 7.3.3*

Policy Compliance Officer	Anita Mathews, Cyber Security Assurance Lead
Policy Manager	Chief Operating Officer
Approval Authority	Senior Executive Team
Review Date	1 April 2032

REVISION HISTORY *(to be completed by Risk, Compliance and Audit)*

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
	Approved	17/09/2026	Senior Executive Team	SET 54/2026	Circular Resolution (05/26), effective 27 August 2026 (previously *Information Security & Information Communication*

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
					Technology (ICT) Appropriate Use Policy)