Cyber Security Procedures

1. COMPLIANCE OBLIGATION SUPPORTED

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

2. PROCEDURAL DETAILS

2.1. Cyber security is key to enabling University Learning and Teaching, Research and Curtin operations. ICT asset users at all levels of the University have specific responsibilities for the management and handling of information and ICT assets. This is essential for achieving, maintaining, and enhancing the University's competitive advantage, brand and reputation, and legal and regulatory compliance.

This document outlines the cyber security responsibilities for members of the University community in any location or campus, whether in or outside of Australia.

2.2. The specific cyber security responsibilities of ICT asset users are dependent on their role within the University and are outlined in these Procedures.

2.3. **Executive Managers**

2.3.1. Executive Managers will champion and support the University's cyber security strategy and programs to reduce Curtin's cyber risk to agreed risk appetite levels.

2.3.2. Executive Managers will allocate sufficient resources and budget, commensurate with the evolving risk of cyber security threats to the University to continually mature Curtin's cyber security capabilities.

2.3.3. Executive managers will promote cyber security culture across Curtin to reduce the risk of cyber impact to Curtin and promote positive behaviours and engagement.

2.4. **Chief Information Officer (CIO)**

2.4.1. The Chief Information Officer (CIO) will ensure the effective and efficient delivery of ICT services to the University that is consistent with the University's cyber security risk appetite and other legislative requirements.

2.4.2. The CIO will allocate sufficient resources and support for the management of cyber security, including the protection of ICT assets.

2.5. **Chief Information Security Officer (CISO)**

2.5.1. The CISO, or their nominated delegate, will approve and direct all cyber security related matters. This includes but is not limited to:

(a) Cyber security policy development and management
(b) Cyber security governance and compliance
(c) Cyber security awareness initiatives
(d) Cyber security incident response management
(e) Cyber security investigations
(f) Cyber security threats and vulnerability management.

2.5.2. The CISO will:

(a) Act as the University's representative when dealing with law enforcement agencies, other universities, and government agencies with respect to cyber security matters.
(b) Assist Executive Management in defining the scope and support required for the University's cyber security Program.
(c) Assist the Chief Information Officer and Executive Management in defining the University's cyber security threat landscape and cyber security risk appetite.

2.5.3. The CISO will establish and maintain cyber security standards that relevant ICT assets will adhere to and with authorise exceptions, where sufficient justification is provided.

2.6. **ICT Asset Users**

2.6.1. ICT asset users will report any cyber security threats or incidents, vulnerabilities or identified weaknesses to the Curtin DTS Service desk and will report any threat or incident involving personal or sensitive information in accordance with the Information Breach Procedures.

3. RESPONSIBILITIES

Responsibilities are as set out in Section 2.

4. SCOPE OF PROCEDURES

These procedures apply 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 or 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 purposes 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.

6. SCHEDULES

Nil

7. RELATED DOCUMENTS/LINKS/FORMS

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	Chief Operating Officer
Review Date	1st April 2030

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

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
New	Approved	22/03/2021	Chief Operating Officer	EM2142	
	Approved	27/10/2026	Chief Operating Officer	EM2617	Previously titled "*Information Security Procedures*"