Information Security Procedure

1 STRATEGIC PLAN THEME AND COMPLIANCE OBLIGATION SUPPORTED

Strategic Plan Theme: People and Culture

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

2 PROCEDURAL DETAILS

This document outlines the information security responsibilities for University staff, adjuncts, associates, students, contractors and consultants in any location or campus, whether in or outside of Australia.

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

3 RESPONSIBILITIES

The specific information security responsibilities of staff and students are dependent on their role within the University and are outlined in this procedure.

3.1 Executive Managers

3.1.1 Executive Managers will champion and support the University's information security program that would enable the University to achieve its strategic objectives.

3.1.2 Executive Managers will allocate sufficient budget, commensurate with the evolving risk of Information Security threats to the University.

3.2 Chief Information Officer

3.2.1 The Chief Information Officer will ensure the effective and efficient delivery of ICT to the University that is consistent with the University's information security risk appetite and other legislative requirements.

3.2.2 The Chief Information Officer will allocate sufficient resources and support for the management of information security, including the protection of ICT Assets.

3.3 Chief Information Security Officer

3.3.1 The Chief Information Security Officer will enable the University to achieve its strategic objectives in an appropriate and responsible manner while ensuring the University maintains a risk-appropriate information security posture.

3.3.2 The Chief Information Security Officer will establish and maintain the University's Information Security Strategy and the supporting Information Security Program.

3.3.3 The Chief Information Security Officer is the authorised representative of Curtin to approve and direct all information security related matters. This includes but is not limited to:

(a) Information Security incident management

(b) Information Security investigations

(c) Cyber Security breach investigations

(d) Information Security awareness initiatives.

3.3.4 The Chief Information Security Officer will:

(a) act as the University's representative when dealing with law enforcement agencies, Universities and government agencies with respect to Information Security matters

(b) assist Executive Management in defining the scope and support required for the University's Information Security Program

(c) assist the Chief Information Officer and Executive Management in defining the University's Information Security threat landscape and information security risk appetite.

3.3.5 The Chief Information Security Officer will establish and maintain information security standards that relevant ICT Assets will adhere to.

3.4 Manager, Cyber Security Operations

3.4.1 The Manager, Cyber Security Operations will deliver the University's supporting Information Security Program and advice the Chief Information Security Officer on the University's Information Security Strategy.

3.4.2 The Manager, Cyber Security Operations is the authorised representative of Curtin to approve, direct, and advise on all operational information security related matters. This includes but is not limited to:

(a) Information Security incident management

(b) Information Security investigations

(c) Cyber Security breach investigations.

3.5 Information Asset Owners

3.5.1 All Information Assets will have a designated Information Asset Owner.

3.5.2 The Information Asset Owner will ensure effective information security controls are implemented for Information Assets using a risk-based approach and act as authority in making decisions in relation to Information Assets.

3.5.3 The Information Asset Owner will ensure Information Assets are appropriately classified per the University's Information Security Classification Policy.

3.5.4 The Information Asset Owner will ensure access to Information Assets is appropriate and authorised.

3.6 Information Asset Administrators

3.6.1 All Information Assets will have one or more designated Information Asset Administrators.

3.6.2 The Information Asset Administrators are responsible for implementing information security controls to an Information Asset and ensuring they are commensurate with the information security classification and the risk profile of the Information Asset and to seek guidance from the Curtin Information Security Team when controls proposed from Information Asset Owners do not adequately meet these criteria.

3.6.3 The Information Asset Administrators will ensure appropriate approval from the Information Asset Owner or their authorised representative, is received prior to allowing access to, modification, disclosure or destruction of an Information Asset by an Information Asset User.

3.7 Information Asset Users

3.7.1 The Information Asset Users will report any information security vulnerabilities or identified weaknesses to the Curtin Information Security Team.

4 SCOPE OF PROCEDURES

These procedures apply to staff, adjuncts, University Associates, students, contractors and consultants in any location or campus, whether in or outside of Australia 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.

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

Controls
Technical or administrative safeguards or countermeasures to avoid, detect, counteract, or minimise information security risks to the University's physical property, Information Assets, ICT Assets or personnel.

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 Assets
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 & Technology Solutions) 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 University staff, adjuncts, associates, students, contractors and consultants in any location or campus, whether in or outside of Australia 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.

Manager, Cyber Security Operations
As defined by University role, or in the alternative, the contracted IT Security Manager or equivalent position in offshore locations.

SCHEDULES

Nil

6 RELATED DOCUMENTS/LINKS/FORMS

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 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	Robbie Whittome, Chief Information Security Officer, Digital & Technology Solutions
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2024

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
1	Approved	22/03/2021	Chief Operating Officer	EM2142	