Information Breach Procedures

1. COMPLIANCE OBLIGATION SUPPORTED

Information Breach Policy

2. PROCEDURAL DETAILS

This document outlines procedures to ensure that the University community responds to any information breach in a timely and effective manner, minimizing any potential harm to individuals and the University.

Any actual or potential unauthorised access, modification, loss or disclosure to personal information and sensitive personal information held by the University (including third parties such as contractors) will be reported in accordance with these Procedures.

2.1 Responsibilities

Refer below.

2.2 Preventing Information Breaches

When entering into any new service, system, project or agreement with any third party in which personal information or sensitive personal information will be used, shared, accessed or disclosed; the appropriate area representative will ensure that appropriate security measures are established as contractual obligations.

2.3 In the event of an Information Breach

Members of the University community are responsible for advising their line manager or supervisor (if applicable) and the University Privacy Officer of any actual or potential information breach incident.

2.3.1 Reports must be made in a timely manner regardless of the scope or impact of the incident.

2.3.2 Information breach incidents which relate to research data must also be reported to the Director, Research Services and Systems.

2.4 Managing an Information Breach

2.4.1 The Privacy Officer must notify all relevant stakeholders in accordance with the *risk rating* for the incident.

2.3.2 Where relevant, cybersecurity processes ,consistent with the Information Security Procedures will be enacted to contain the breach in a timely manner.

2.3.3 Information breach incidents will be recorded in an Information Breach Register by the Privacy Officer responsible for the incident.

2.3.4 Parties affected by an information breach incident must be informed of the incident and the progress of any investigation in a timely manner.

2.3.5 Where an individual is personally impacted by an incident, that individual must be informed in writing without undue delay by the Privacy Officer, including advice on mitigating risk to themselves and will be advised of actions taken to address the incident.

2.3.7 The Privacy Officer must collaborate with appropriate stakeholders to coordinate a formal plan to respond to the incident in accordance with the *Incident Alert Matrix* and risk rating.

2.3.10 The Privacy Officer responsible for the incident must document the incident in the Information Breach Register, including the cause, any processes or mitigation measures recommended, the number of impacted individuals, whether the incident was deemed a notifiable incident and the time taken to investigate.

2.3.12 The Privacy Officer responsible for the incident must notify affected parties of the outcome of the investigation.

3 SCOPE OF PROCEDURES

This procedure applies to the University Community, including Council members, students, staff, University Associates, Curtin controlled entities, and all persons participating in University business or activities, including whether as a visitor, adjunct appointee, service provider, contractor or volunteer. Global campuses must abide by freedom of information, privacy and any requirements for the management and reporting of data breaches which apply to their jurisdiction.

4 DEFINITIONS

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

Information Breach
Any unauthorised access to personal information or sensitive personal information, or any unauthorised or accidental disclosure of personal information or sensitive personal information, or any loss of personal information or sensitive personal information which is likely to result in serious harm to any individual.

Sensitive personal information

A classification of personal information that includes a person's racial or ethnic origin; political opinions or memberships of a political association; religious or philosophical beliefs or affiliations; membership of a professional or trade association or union; sexual orientation or practices; criminal records; genetic, health or biometric information.

3. RELATED DOCUMENTS/LINKS/FORMS

- Curtin Information Statement
- *Privacy Policy*
- *Privacy Procedure*
- *Information and Communication Technology (ICT) Appropriate Use Procedures*
- *Information Management Policy*
- *Information Security and Information and Communication Technology (ICT) Appropriate Use Policy*
- Information Security Classification Decision Matrix
- Information Security Classification Flowchart
- *Information Security Classification Policy*
- Investigate a Privacy Data Breach
- Privacy Advice – Student Confidentiality
- *Research Data and Primary Materials Policy*
- Student's Privacy Collection Notice
- Australian Privacy Principles
- *Criminal Code Act Compilation Act 1913* (WA)

- *Electronic Transactions Act 2011* (WA)
- *Evidence Act 1906* (WA)
- *Freedom of Information Act 1992* (WA)
- *Privacy Act 1988* (Cth)
- *State Records Act 2000* (WA)
- *Privacy and Responsible Information Sharing Act* (WA)

Policy Compliance Officer	Krista Bell, Director, Data & Information Governance
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2028

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

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
	Approved	19/12/2024	Chief Operating Officer	EM2434	