Data Breach Response Procedures

INTRODUCTION

Strong data management is integral to the successful operation of the University. The University is committed to protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The University has an ongoing obligation to take steps to handle personal information in accordance with the *Australian Privacy Principles*.

The University Community have to trust that their privacy is protected and be confident that personal information is secured in line with their expectations.

COMPLIANCE

This is a compliance requirement under the *Privacy Act 1988 (Commonwealth).*

INTENT

This document outlines the procedure for the University to follow in the event of an identified eligible data breach occurring.

RELEVANT DEFINITIONS

In the context of this document:

Australian Privacy Principles means the principles that set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information as contained in Schedule 1 of the *Privacy Act*;

Eligible data breach means a breach of personal data security that is likely to result in serious harm to any of the individuals to whom the data relates, and the University has been unable to prevent the likely risk of serious harm with remedial action;

Eligible Data Breach Response Team means the University's Privacy Officer, Chief Information Officer, Director Media and Communications and the relevant senior manager of the organisational unit where the potential eligible data breach occurred plus any other relevant staff members given the circumstances;

Loss means the accidental or inadvertent loss of personal information held by the University, in circumstances where is it is likely to result in unauthorised access or disclosure. An example is where a staff member leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport;

Organisational unit means a school, college, centre or other academic unit, a department, or other administrative unit;

Personal information means information such as name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about an identified individual or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not;

Privacy Officer means the staff member of the University who is responsible for ensuring that the University collects, manages, uses and discloses personal information in a compliant manner. Currently the Director, Strategic Services and Governance is the University's Privacy Officer;

Reasonably identifiable means whether a person can be identified from available information, and the process of identification is reasonable to achieve, this may vary from situation to situation;

Senior manager means a staff member of the University holding the position of College Dean, Head of School or Director;

Serious harm means, in the context of a data breach, serious harm to an individual that may include serious physical, psychological, emotional, financial, or reputational harm;

Staff member means anyone employed by the University and includes all continuing, fixed-term, casual, adjunct or honorary staff or those holding University offices or who are a member of a University committee;

Unauthorised access means when personal information, that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by a staff member, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, a staff member browses sensitive customer records without any legitimate purpose, or a computer network is compromised by an external attacker, resulting in personal information being accessed without authority;

Unauthorised disclosure means when the University, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the University, and releases that information from its effective control in a way that is not permitted by the *Privacy Act*. This includes an unauthorised disclosure by a staff member of the University. For example, accidental publication of a confidential data file containing the personal information of one or more individuals on the internet; and

University Community means officials and individuals carrying out University business. This includes, but is not limited to, all staff members, researchers, peer reviewers, students, volunteers, consultants, agents and contractors.

PROCEDURES

Suspected or known data breach

A data breach is a breach of personal data security that is likely to result in serious harm to any of the individuals to whom the data relates.

When a real or potential data breach is identified the Privacy Officer must be informed immediately.

Assess

The Eligible Data Breach Response Team must consider whether the data breach is likely to be classified as an eligible data breach. The Privacy Officer must consider reporting the identified data breach to relevant law enforcement agencies and then act on any advice received regarding further investigation and reporting obligations.

An eligible data breach is a breach of personal data security that is likely to result in serious harm to any of the individuals to whom the data relates, and the University has been unable to prevent the likely risk of serious harm with remedial action; as described by the *Office of the Australian Information Commissioner*.

Based on the assessment of the data breach, if the Eligible Data Breach Response Team has reasonable grounds to believe that an eligible data breach has occurred, a decision must be made to notify the Australian Information Commissioner.

The Eligible Data Breach Response Team will follow the recommendations of the Australian information Commissioner by:

- Investigating and gathering relevant information about the incident to determine what has occurred. In particular seeking information about what data has been breached, shared with whom and who is affected; and
- Evaluating and making evidence based decision about whether serious harm is likely. This process must be fully documented.

The assessment must be conducted where possible within thirty (30) days of the breach. If this can not be done, the Privacy Officer must document the reasons why.

Contain

After assessing the data breach, the Eligible Data Breach Response Team must ensure that the necessary steps to contain any suspected or known data breaches where possible are being implemented. This means taking immediate action to limit any further access or distribution of the affected personal data, or the possible compromise of other data.

Take remedial action

Where possible the Privacy Officer must initiate steps to reduce any potential harm to individuals.

This involves taking action to recover lost data before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm to individuals no longer likely, then notification to the Australian Information Commissioner is not mandatory. The Privacy Officer can progress to a review of the data breach without having to notify the Australian Information Commissioner of the data breach.

Notification of eligible data breach

The Privacy Officer must notify the affected individuals that the notification of a potential eligible data breach has been lodged with the Australian Information Commissioner, and inform them of the contents.

The Privacy Officer will use one of three options for notification of data Breaches depending on the circumstances. They will either:

- Notify all individuals involved in the data breach;
- Notify only those individuals at risk of serious harm as a result of the data breach; or
- Publish the statement on the University's website and publicise it, if the previous methods of notification are not practical.

The Privacy Officer may provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

Where serious harm is likely, the Privacy Officer will prepare a statement for lodgement with the Australian Information Commissioner. The statement must contain:

- The University's contact details
- A description of the breach;
- The kind of information concerned; and
- Recommended steps for the individuals affected.

Review

Following the notification of a potential eligible data breach and any corrective action being taken, the Eligible Data Breach Response Team must review the incident and initiate action to prevent future data breaches. This includes:

- Fully investigating the cause of the breach;
- Developing a prevention plan to safeguard against future data beaches;
- Conducting audits to ensure the prevention plan is correctly implemented;
- Updating security/response plan;
- Considering changes to policies and procedures; and
- Revising staff training practises.

ESSENTIAL SUPPORTING INFORMATION

Internal

Code of Conduct

Critical Incident Policy

Information Communication Technologies Acceptable Use Policy

Privacy and Confidentiality Policy

Risk Management Policy

External

Privacy Act 1988 (Commonwealth)

Australian Privacy Principles

Document History and Version Control			
Last amendment:	19 Sep 2018	**Next Review:**	19 Sep 2020
Sponsor:	Director Strategic Services and Governance		
Contact Officer:	Director Strategic Services and Governance		

Version	Date Approved	Approved by	Brief Description
1.00	19 Sep 2018	Vice-Chancellor	Creation of original document and upload to CDU website.