Name of Procedure	Data Breach Procedure & Response Plan
Governing Policy	Privacy Policy
Description of Procedure	This Procedure sets out the processes to be followed by ACU staff in the event that ACU experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.
Policy applies to	☒ University-wide ☐ Specific (*outline location, campus, organisational unit etc.)*
	☒ All Staff ☒ All Students ☒ Third Parties
Procedure Status	☒ New Procedure ☐ Revision of existing procedure

Approval Authority	Vice-Chancellor and President
Governing Authority	Chief Operating Officer
Responsible Officer	Director, Governance

Approval Date	18 December 2017
Effective Date	1 January 2018
Approval Date of Last Revision	
Effective Date of Last Revision	
Date of Policy Review*	1 January 2020

** Unless otherwise indicated, this procedure will still apply beyond the review date.*

DATA BREACH PROCEDURE & RESPONSE PLAN

1. Policy

This Procedure is governed by the Australian Catholic University (**ACU**) *Privacy Policy*.

2. Introduction

ACU is committed to managing personal information in accordance with the *Privacy Act 1988 (Cth)* (the Act) and the ACU Privacy Policy.

This document sets out the processes to be followed by ACU staff in the event that ACU experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, ACU needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

Adherence to this Procedure and Response Plan will ensure that ACU can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's *"Guide to developing a data breach response plan*"
- The Office of the Australian Information Commissioner's *"Data breach notification guide: a guide to handling personal information security breaches*"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with *ACU's Privacy Policy*.

3. Process where a data breach occurs or is suspected

3.1. Alert

Where a privacy data breach is known to have occurred (or is suspected) any member of ACU staff who becomes aware of this must, within 24 hours, alert a Member of the Executive in the first instance.

Note: the term 'Member of the Executive' is defined in ACU's Delegation of Authority Policy.

The Information that should be provided (if known) at this point includes:

a) When the breach occurred (time and date)
b) Description of the breach (type of personal information involved)
c) Cause of the breach (if known) otherwise how it was discovered
d) Which system(s) if any are affected?
e) Which directorate/faculty/institute is involved?
f) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

A template can be found at **Annexure A** to assist in documenting the required information.

3.2. Assess and determine the potential impact

Once notified of the information above, the Member of the Executive must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The Privacy Coordinator should be contacted for advice.

3.2.1 Criteria for determining whether a privacy data breach has occurred

a) Is personal information involved?
b) Is the personal information of a sensitive nature?
c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

For the purposes of this assessment the following terms are defined in section 9 of the *Privacy Policy:* personal information, sensitive information, unauthorised access, unauthorised disclosure and loss.

3.2.2 Criteria for determining severity

a) The type and extent of personal information involved
b) Whether multiple individuals have been affected
c) Whether the information is protected by any security measures (password protection or encryption)
d) The person or kinds of people who now have access
e) Whether there is (or could there be) a real risk of serious harm to the affected individuals
f) Whether there could be media or stakeholder attention as a result of the breach or suspect breach

With respect to 3.2.2(e) above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in section 9 of the *Privacy Policy* and section 26WG of the NDB Act.

Having considered the matters in 3.2.1 and 3.2.2, the Member of the Executive must notify the Privacy Officer within 24 hours of being alerted under 3.1.

3.3 Privacy Officer to issue pre-emptive instructions

On receipt of the communication by the relevant member of the Executive under 3.2, the Privacy Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, the Privacy Officer will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This will depend on the nature and severity of the breach.

3.3.1 Data breach managed at the Directorate/Faculty/Institute level

Where the Privacy Officer instructs that the data breach is to be managed at the local level, the relevant Member of the Executive must:

- ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and

- submit a report via the Privacy Coordinator within 48 hours of receiving instructions under 3.3. The report must contain the following:

    - Description of breach or suspected breach
    - Action taken
    - Outcome of action
    - Processes that have been implemented to prevent a repeat of the situation.
    - Recommendation that no further action is necessary

The Privacy Officer will be provided with a copy of the report and will sign-off that no further action is required.

The report will be logged by the Privacy Coordinator.

3.3.2 Data breach managed by the Response Team

Where the Privacy Officer instructs that the data breach must be escalated to the Response team, the Privacy Officer will convene the Response Team and notify the Vice-Chancellor and President.

The Response team will consist of:

- Privacy Coordinator
- General Counsel (or nominee)
- Director of Human Resources (or nominee)
- Academic Registrar (or nominee)
- Director of Information Technology (or nominee)
- Director of Marketing and External Relations (or nominee)

3.4. Primary role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

- Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
- evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 3.2.1 and 3.2.2 above.
- Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
- Engage an independent cyber security or forensic expert as appropriate.
- Assess whether serious harm is likely (with reference to section 3.2.2 above and section 26WG of the NDB Act).
- Make a recommendation to the Privacy Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.
- Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The Privacy Officer will provide periodic updates to the Vice-Chancellor as deemed appropriate.

3.5. Notification

Having regard to the Response team's recommendation in 3.4 above, the Privacy Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred.

If there are reasonable grounds, the Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

A template can be found at **Annexure B**.

If practicable, ACU must also notify each individual to whom the relevant personal information relates. Where impracticable, ACU must take reasonable steps to publicise the statement (including publishing on the website).

The prescribed statement will be logged by the Privacy Coordinator.

3.6. Secondary Role of the Response Team

Once the matters referred to in 3.4 and 3.5 have been dealt with, the Response team should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.
- Prepare a report for submission to Senate.
- Consider the option of an audit to ensure necessary outcomes are effected and effective.

4. Updates to this Procedure

In line with the University's Policy Development Policy, this procedure is scheduled for review every five years or more frequently if appropriate.

5. Revisions made to this Procedure

Date	Major, Minor or editorial	Description

6. Contact details

Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows:

Privacy Coordinator
E: privacy@acu.edu.au
W: www.acu.edu.au/policy/governance/privacy_policy_and_procedure
T: 02 9465 9151
P: PO Box 968, North Sydney NSW 2059