Procedure: Data breach response plan

Purpose

To set out procedures to implement the mandatory notifiable data breaches scheme that applies under the *Privacy Act 1988*.

Definitions

Data breach means unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information. Examples of a data breach are when a device containing personal information is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.

Notifiable data breach means a data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner.

Personal information means information or an opinion about an individual who is identified, or who can reasonably be identified, from the information, whether or not the information or opinion is true or recorded in a material form, and includes sensitive information; and

Sensitive information means information or an opinion that is also personal information, about a person's racial or ethnic origin, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practises, criminal history, health information, and genetic and biometric information.

Procedure

Identification of a breach

1. ANU experiences data breach or a data breach is suspected: This may be discovered by an ANU staff member, or an ANU staff member may be alerted by another party or system.

2. When an ANU staff member discovers a known or suspected data breach they should immediately notify the ANU Privacy Officer. Please provide as much information as possible such as the time and date the known or suspected breach was discovered, the

type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

3. Any immediate steps available to contain the breach must be identified and implemented in discussion with the Privacy Officer. Reducing the scale and impact of a data breach can prevent the need for notification to the OAIC. All known or suspected data breaches must still be notified internally to the ANU Privacy Officer.

Assessment of a breach

4. Not all data breaches are notifiable. If, after an initial investigation, the Privacy Officer suspects a notifiable data breach may have occurred, a reasonable and expeditious assessment must be undertaken to determine if the data breach is likely to result in serious harm to any individual affected.

5. The ANU Privacy Officer will seek information to assess the suspected breach. In assessing a suspected breach, the Privacy Officer may require assistance and information from other areas of the University depending on the circumstances. For example, a system suspected breach will be investigated by the IT Security Manager, Cyber & Digital Security together with the Privacy Officer and a non-system suspected breach will be investigated Privacy Officer.

6. There will then be an evaluation of the scope and possible impact of the breach. The Privacy Officer will assess if a breach is likely to be notifiable and ensure appropriate actions including reporting to the Office of the Australian Information Commissioner (OAIC). An assessment of a known or suspected breach must be conducted expeditiously and where possible should be completed within 30 days.

7. In all cases the assessment will identify what actions must be taken. These will be documented and acted upon as soon as possible.

8. There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

9. There are four key steps to consider when responding to a breach or suspected breach.

a. STEP 1: Contain the breach and do a preliminary assessment

a. STEP 2: Evaluate the risks associated with the breach

b. STEP 3: Notification to OAIC and affected individuals

c. STEP 4: Prevent future breaches

A notifiable breach

10. A breach which is assessed as likely to result in serious harm to individuals whose personal information is involved, is a notifiable data breach. Such data breaches must be notified to the affected individuals and the OAIC. Notice must include information about the breach and the steps taken in response to the breach.

11. If the University has responded quickly to the breach, and as a result of this action the data breach is not likely to result in serious harm, there is no need to notify individuals or the OAIC. However the University may decide to tell the affected individuals about the incident if it is considered appropriate.

12. The risk of serious harm will be assessed by considering both the *likelihood* of the harm occurring and the *consequences* of the harm. Some of the factors that should be considered are:

Factors	**Considerations**
The type of personal information involved in the data breach.	Some kinds of personal information are more sensitive than others and could lead to serious ramifications for individuals if accessed. Information about a person's health, documents commonly used for identity fraud (e.g. Medicare card, driver's licence) or financial information are examples of information that could be misused if the information falls into the wrong hands.
Circumstances of the data breach	The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to a large number of individuals would normally lead to an overall increased risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant. Consideration must be given to who may have gained unauthorised access to information, and what their intention was (if

	any) in obtaining such access. It may be that there was a specific intention to use the information in a negative or malicious way.
Nature of possible harm	Consider the broad range of potential harm that could follow from a data breach including: identity theft financial loss threat to a person's safety loss of business or employment opportunities and damage to reputation (personal and professional).

13. Notification to the OAIC and internally within the university is the responsibility of the Privacy Officer.

14. Notification to individuals may be undertaken by the Privacy Officer or a University officer in the area in which the breach occurred after the Privacy Officer agrees to the action.

15. Notifications will follow the format identified by the OAIC in *Data breach preparation and response*.

Response team

16. A response team will be formed for a serious breach. The team will include the IT Security Manager, Cyber & Digital Security and an officer from the line area. Staff from the Legal Office and Strategic Communication and Public Affairs Office will provide advice.

17. The Chief Operating Officer will be informed when a Response Team is established.

Breaches that are not serious

18. Breaches that are not assessed as serious breaches may be handled by line managers, but must be reported to the Privacy Officer.

Records

19. Documentation will be stored in the Electronic Records Management System for each suspected breach.

Document information

Title	Data breach response plan
Document Type	Procedure
Document Number	ANUP_017613
Version	3
Purpose	To set out procedures to implement the mandatory notifiable data breaches scheme that applies under the Privacy Act 1988.
Audience	Staff, Students, Prospective Staff, Prospective Students
Category	Administrative
Topic	Information Management
Subtopic	Privacy
Effective Date	15 Mar 2018
Review Date	15 Mar 2021
Responsible Officer	University Librarian and Director, Scholarly Information Services (director.sis@anu.edu.au)
Approved By	Chief Operating Officer (COO@anu.edu.au)
Contact Area	ANU Advancement (felicity.gouldthorp@anu.edu.au)
Authority	Privacy Act 1988
Printed On	29 Nov 2021