Data Breach Management Procedure

Version	Approved by	Approval date	Effective date	Next full review
1.0	Vice-President, Finance and Operations	13 December 2018	13 December 2018	December 2021

Procedure Statement		
Purpose	This *Data Breach Management Procedure* sets out procedures and clear lines of authority for UNSW Sydney staff if UNSW experiences a data breach (or suspects that a data breach has occurred). It should be read in conjunction with the UNSW *Data Breach Policy*.	
Scope	This procedure applies to academic staff, professional staff, students, contractors, consultants, or other agents of the University.	
Are Local Documents on this subject permitted?	☐ Yes, however Local Documents must be consistent with this University-wide Document	☒ No
Procedure Processes and Actions		

Contents

1. Introduction

This *Data Breach Management Procedure* (DBMP) sets out the procedure to be followed by UNSW staff if UNSW experiences a data breach or suspects that a data breach has occurred.

A data breach occurs when personal information held by UNSW is lost or subjected to unauthorised access, modification, use or disclosure or other misuse or interference. Personal information refers to information that identifies or reasonably identifies an individual.

A data breach will also occur where protected UNSW information is unlawfully used or disclosed. This includes a broader range of information than 'personal information' as it includes information about all entities, not just individuals.

It is also important to note that the Office of the Australian Information Commissioner (OAIC) is only concerned with breaches that involve personal information. Data breaches that involve UNSW information that is not 'personal information' do not need to be reported to the OAIC.

Adherence with the Data Breach Response Plan (DBRP) will ensure the UNSW can contain, assess and respond to data breaches in a timely fashion in order to mitigate potential harm to affected persons.

This procedure:

- sets out the roles and responsibilities of staff
- provides a link to the details of appropriate staff that should be contacted in the event of a data breach
- outlines the procedure to be followed in the event of a data breach.

1.1. Initial Response

A staff member who has identified a suspected data breach should immediately notify their Faculty or Division Liaison person.

The notification must include information about the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.

A list of Faculty or Divisional Liaison people is available here:
https://www.datagovernance.unsw.edu.au/node/10

1.2. Faculty or Divisional Liaison person to assess the breach

The Liaison person for the Faculty or Division must assess and determine whether a data breach has occurred.

If they have any suspicion that a breach has occurred, then they must immediately raise a ticket via the IT Service Centre (email itservicecentre@unsw.edu.au).

1.3. Data Breach Management Committee to assess the seriousness of the breach

The Data Breach Management Committee will review the data breach and update the IT ticket accordingly. The ticket shall record:

- the description of the breach or suspected breach
- the action taken by UNSW staff to address the breach or suspected breach
- the outcome of that action
- agreement from the Data Breach Management Committee that no further action is required
- confirmation that the incident has been recorded as a data breach incident log.

1.4. Data Breach Management Committee to refer Breach to UNSW IT Cyber Security

In the event that a data breach has been established, the Data Breach Management Committee will refer the matter to the UNSW IT Cyber Security team for action. The Cyber Security team will report on progress to the Data Breach Management Committee.

2. Data Breach Management Committee

Membership of the Data Breach Management Committee includes (but is not limited to):

- Chief Data & Analytics Officer (UNSW Planning & Performance) – Committee Chair
- Chief Information Security Officer (UNSW IT)
- Director of Risk Management (Division of Strategy & Quality)
- Director of Customer Service Delivery (UNSW IT)
- Privacy Officer (Legal)
- Head of Media (Division of External Relations)
- Head of Digital (Division of External Relations).

Note: It is not necessary that all members of the Data Breach Management Committee be included in all data breach responses. However, where a Division/Faculty is affected or involved in a breach, or where a Division/Faculty can assist in mitigating the harm caused by a breach, a listed or delegated primary or secondary contact must be involved in the response.

The Committee is responsible for decisions, in consultation with UNSW Data Owners, regarding notification of individuals who have been impacted in the data breach. The Committee will consider the following factors:

- The risk of harm to the individual/organisation
- Steps that UNSW has taken to date to avoid or remedy any actual or potential harm
- The ability of the individual/organisation to take further steps to avoid or remedy harm
- Whether the information that has been compromised is sensitive, or likely to cause humiliation or embarrassment for the individual/organisation

- Whether there are any applicable legislative provisions or contractual obligations that require UNSW to notify affected individuals and other parties (e.g. Privacy Commissioner).

A record of the response must be saved in the IT Service Desk ticket relevant to the data breach.

If the breach is serious, it must immediately be escalated to the Data Breach Management Committee.

2.1. Process

Once a matter has been escalated to the Data Breach Management Committee, the process outlined below must be followed. The Data Breach Management Committee must work in consultation with the Executive in responding to the breach. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances.

There are four key steps to consider when responding to a breach or suspected breach. Generally, steps 1-3 should be carried out concurrently or in close succession.

- Step 1: Contain the breach and do a preliminary assessment
- Step 2: Evaluate the risks associated with the breach
- Step 3: Notification
- Step 4: Prevention of future breaches.

These steps are described in more detail in the following subsections.

2.1.1 Contain the breach and conduct a preliminary assessment

Contain the breach

Once a data breach has been identified, action must be taken to immediately contain it. For example, stop the unauthorised practice, recover the records or shut down the system that was breached.

Initiate a preliminary assessment

Move quickly to appoint someone to lead the initial investigation. This person must be suitably qualified and have sufficient authority to conduct the initial investigation. In some instances, this may be a member of the Data Breach Management Committee. In other instances, it will be a person most suitably qualified to carry out the initial investigation (as determined by the members of the Data Breach Management Committee).

In some situations, it will be necessary to assemble a team that includes representatives from appropriate areas of the UNSW to conduct the preliminary assessment.

The following questions should be addressed when making the preliminary assessment:

- What information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to affected persons) that could potentially be caused by the breach?
- How can the breach be contained?

2.1.2 Evaluate the risks associated with the breach

The following factors are relevant when assessing the risk by the Data Breach Management committee:

- The type of information involved
- Whether it is personal information or protected UNSW information
- Whether the type of information that has been compromised creates a greater risk of harm
- Who is affected by the breach.

Determine the context of the affected information and the breach

- What is the context of the information involved?
- What parties have gained unauthorised access to the affected information?
- Have there been other breaches that could have a cumulative effect?

  How could the information be used?

Establish the cause and extent of the breach

- Is there a risk of ongoing breaches or further exposure of the information?
- Is there evidence of theft?
- Is the information adequately encrypted, anonymised or otherwise not accessible?
- What was the source of the breach? (risk of harm may be lower where source of the breach is accidental rather than intentional)
- Has the information been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?
- How many persons are affected by the breach?

Assess the risk of harm to the affected persons

- Who is the recipient of the information?
- What harm to persons could result from the breach?

Assess the risk of other harms

Assess other possible harms, including to the agency or organisation that suffered the breach. For example:

- The loss of public trust in the agency
- Reputational damage
- Legal liability
- Breach of secrecy provisions.

A thorough evaluation of the risks will assist the UNSW in determining the appropriate course of action to take.

2.1.3 Notification

Deciding whether to notify affected individuals or entities

In general, if the Data Breach Management Committee determines that the data breach creates a real risk of serious harm to a person, the affected person should be notified.

The Data Breach Management Committee will take as its key consideration whether notification is necessary to avoid or mitigate serious harm to an affected person.

In coming to this the decision, the Data Breach Management Committee will consider the following factors:

- What is the risk of serious harm to the person as determined by the evaluations of the risks associated with the breach?
- What is the ability of the person to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)?
- Even if the person would not be able to take steps to fix the situation, is the information that has been compromised sensitive or likely to cause humiliation or embarrassment?
- What are the legal and contractual obligations to notify and what are the consequences of notification?

Notification process

- In general, notification should occur as soon as reasonably possible. However, in some instances, delay may be necessary

- Notification should be direct – by phone, letter, email or in person, to the affected individuals
- Indirect notification, either by website, posted notices or media may be used only where direct notification could cause further harm, is cost prohibitive or the contact information for affected persons is unknown.

Details to include in the notification

The content of the notification will vary depending on the particular breach and notification method, but where relevant will include:

- incident description
- type of information involved
- response to the breach
- assistance offered to affected persons
- other information sources designed to assist in protecting against identity theft or interferences with privacy (e.g. www.oaic.gov.au).
- the UNSW's contact details
- whether the breach has been notified to the regulator or other external contact(s) and the legal implications (e.g. the secrecy provisions)
- how individuals can lodge a complaint with the UNSW
- how individuals can lodge a complaint with the OAIC (where the information is personal information).

Other notifications

The Data Breach Management Committee will also determine if it is appropriate and necessary to notify other third parties, such as:

- The OAIC
- The Police
- Insurance providers
- Credit card companies and/or financial institutions
- Professional or other regulatory bodies
- Other internal or external parties who have not already been notified
- Agencies that have a direct relationship with the information lost/stolen.

In determining whether it is appropriate and necessary to notify OAIC the Data Breach Management Committee will consider the following factors:

- any applicable legislation that may require notification
- the type of personal information involved and whether there is a risk of serious harm arising from the breach
- whether a large number of people were affected by the breach
- whether the information was fully recovered without further disclosure
- whether the affected individuals have been notified, and
- if there is a reasonable expectation that the OAIC may receive complaints/inquiries about the breach.

2.1.4 Prevention of future breaches

Once immediate steps have been taken to mitigate the risks associated with a breach, the Data Breach Management Committee must take the time to investigate the cause of the breach.

Following a breach, the Data Breach Management Committee will provide a brief to the UNSW Audit Committee on the outcome of the investigation and relevant recommendations, including:

- making appropriate changes to policies and procedures if necessary

- revising staff training practices if necessary
- updating this Data Breach Management Procedure if necessary.

3. References

This Data Breach Management Procedure has been developed in accordance with, and with reference to, the OAIC's Data Breach Notification Guide. The Data Breach Management Committee should refer to the guide as it provides further detail that may be of assistance.

Accountabilities	
Responsible Officer	Director, UNSW Planning & Performance
Contact Officer	Chief Data & Analytics Officer (datagov@unsw.edu.au)
Supporting Information	
Legislative Compliance	This policy supports the University's compliance with the following legislation: *Privacy Act 1988* (Cth) *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) *Health Records and Information Privacy Act 2002* (NSW) *Health Records and Information Privacy Code of Practice 2005* (NSW) *Health Records and Information Privacy Regulation 2012* (NSW) *Privacy and Personal Information Protection Act 1998* (NSW) *Privacy and Personal Information Protection Regulation 2014* (NSW)
Parent Document (Policy)	Data Breach Policy
Supporting Documents	Nil
Related Documents	Data Classification Standard Data Governance Policy Data Handling Guidelines Privacy Management Plan IT Security Policy IT Security Standards Data Breach Notification Guide. A guide to handling personal information security breaches
Superseded Documents	Nil
File Number	2018/29892
Definitions and Acronyms	
Constituent	A person in respect of whom UNSW stores personally identifiable information during the normal course of business.
Data Breach	A data breach occurs when personal information held by UNSW is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach may include the loss or theft of a device containing personal information of UNSW constituents, UNSW's database or information repository containing personal information being hacked or accessed without authorisation, or UNSW mistakenly providing personal information to an unauthorised person or entity.
Data Breach Management Committee (DBMP)	Senior personnel at UNSW who are responsible for ensuring that a data breach is managed appropriately.
Data Breach Plan	A framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by UNSW in managing a breach if one occurs.

Data Breach Response Plan (DBRP)	The plan of action that is determined by the Data Breach Management Committee so as to contain and remediate the data breach.
OAIC	Office of the Australian Information Commissioner
Please refer to the Collibra Data Governance Centre (zID and zPass required) and search for up to date definitions (https://unsw.collibra.com).	

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-President, Finance and Operations	13 December 2018	13 December 2018	This is a new Procedure