Data Breach Policy

Version	Approved by	Approval date	Effective date	Next review
1.0	President and Vice-Chancellor	18 April 2018	18 April 2018	April 2021
Policy Statement				
Purpose	To outline the principles for responding to a breach of UNSW held data, including the steps that personnel must use to ensure that data breaches are identified, contained, investigated, and remedied.			
Scope	This policy applies to academic staff, professional staff, students, contractors, consultants, or other agents of the University.			
Policy Provisions				

1. Introduction

This policy describes the principles for responding to a breach of UNSW held data including managing a data breach and notification of persons whose privacy may be affected by the breach. Effective breach management assists UNSW in avoiding or reducing possible harm to both the affected individuals and UNSW and may prevent future breaches.

The policy also describes the principles relating to documentation, appropriate reporting internally and externally, and communication so that organisational learning occurs. It establishes responsibility and accountability for all steps in the process of addressing information security incidents that result in data breaches and describes clear roles and responsibilities with the aim of ensuring a comprehensive and well-managed privacy and information governance program.

Having a data breach response plan is part of establishing robust and effective privacy and information governance procedures, at UNSW this is included in the Data Breach Management Procedure. And having clear roles and responsibilities is the foundation to a comprehensive and well-managed privacy and information governance program. This *Data Breach Policy* assists with:

- Meeting UNSW's obligations under the *Privacy Act 1988* (Cth).
- Protection of an important business asset — the personal information of UNSW's constituents, including but not limited to staff, students, alumni, research subjects — as well as UNSW's reputation.
- Dealing with adverse media or stakeholder attention from a breach or suspected breach.
- Instilling public confidence by responding to a breach systematically and effectively, with the aim of meeting UNSW obligations and protecting business and personal assets.

To enhance robust and effective privacy and Information Governance procedures, a *Data Breach Management Procedure* has also been developed.

2. Data Breach Definition

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, a UNSW 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.

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to UNSW data, such as:

- Accidental loss, unauthorised access, or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to, or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of classified material information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the website without consent
- A compromised user account (e.g. accidental disclosure of user login details through phishing)

- Failed or successful attempts to gain unauthorised access to UNSW information or information systems
- Equipment failure
- Malware infection
- Disruption to or denial of IT services

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

3. Data Breach Response Plan

A Data Breach Response Plan enables UNSW to respond quickly to a data breach. It is 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. The UNSW Data Breach Response Plan is established by the Data Breach Management Committee.

Where a data breach is suspected it is required that UNSW personnel contact the UNSW IT Service Centre (ITServiceCentre@unsw.edu.au) advising of the suspected data breach. The IT Service Centre will then initiate the Data Breach Response Plan using the UNSW *Data Breach Response Procedure*.

4. Data Breach Management

There are five key steps required in responding to a data breach:

1. Contain the breach
2. Evaluate the associated risks
3. Recovery
4. Consider notifying affected individuals and escalation to UNSW senior management
5. Prevent a repeat.

The UNSW person who notifies of a breach shall report it to the IT Service Centre (ITServiceCentre@unsw.edu.au), who will then escalate the matter to the Data Breach Management Committee.

5. Roles and Responsibilities

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

- Chief Data & Analytics Officer (UNSW Planning & Performance)
- 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)

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 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.

Accountabilities	
Responsible Officer	Vice President, Strategy & Quality
Contact Officer	Chief Data & Analytics Officer
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) (HRIP Act) (NSW Legislation website) *Health Records and Information Privacy Code of Practice 2005* (NSW) (NSW Legislation website) Health Records and Information Privacy Regulation 2012 (NSW) (HRIP Regulation) (NSW Legislation website) *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) (NSW Legislation website) Privacy and Personal Information Protection Regulation 2014 (2014-549) (NSW) (PPIP Regulation)
Supporting Documents	Data Breach Management Procedure Data Breach Management Plan
Related Documents	Data Classification Standard Data Governance Policy Data Handling Guidelines IT Security Policy IT Security Standards
Superseded Documents	Nil
File Number	2018/07574
Definitions and Acronyms	
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	Senior personnel at UNSW who are responsible for ensuring that a data breach is managed appropriately.
Data Breach Response Plan	The plan of action that is determined by the Data Breach Management Committee so as to contain and remediate the data breach.
Constituent	A person in respect of whom UNSW stores personally identifiable information during the normal course of business.
Data Owners	Data Owners are responsible for ensuring effective local protocols are in place to guide the appropriate use of their data. Access to, and use of, institutional data will generally be administered by the appropriate Data Owner. They are also responsible for ensuring that data conforms to legal, regulatory, exchange, and operational standards.
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.
Personal Information	Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion

Revision History				
Version	**Approved by**	**Approval date**	**Effective date**	**Sections modified**
1.0	President and Vice-Chancellor	18 April 2018	18 April 2018	This is a new Policy