Data Breach Policy and Procedure

Version	Approved by	Approval date	Effective date
2.0	Vice-Chancellor and President	3 November 2023	3 November 2023

Policy provisions

Purpose

This document sets out the policy principles and procedures for identifying, assessing, managing and responding to a breach of data held by UNSW. It establishes responsibility and accountability for all steps in addressing information security incidents resulting in data breaches and describes clear roles and responsibilities. It also describes the principles and procedures relating to internal and external notification and communication of such data breaches.

Scope

This policy and procedure applies to all UNSW staff, students, contractors, consultants, third-party vendors and agents of the University.

Principles

The following principles guide UNSW staff in identifying, assessing, managing and responding to a breach of data held by UNSW:

1. Data is an important business asset that must be protected.
2. Personal information and health information held by the University is managed in accordance with the Information Protection Principles (IPPs), the Health Privacy Principles (HPPs), and other applicable privacy laws and contractual obligations.
3. A robust data breach management program assists UNSW in complying with its legislative obligations to protect data; avoiding or reducing possible harm to affected individuals and UNSW; and may prevent future breaches.
4. Data breaches are reported as soon as they are identified.
5. Data breaches are assessed and managed systematically and effectively in accordance with the Data Breach Management Plan.
6. Affected individuals and entities are appropriately notified of a data breach in accordance with legislative obligations.
7. Data breaches are accurately recorded to enable UNSW to comply with legislative obligations and monitor, analyse and review the type and severity of suspected data breaches and the effectiveness of its response.
8. UNSW's training in data governance, recordkeeping, privacy and cyber security enables UNSW staff to effectively and efficiently identify, respond to and manage a data breach.

Types of Data Breaches

A data breach occurs when **any** information (whether in digital or hard copy) held by UNSW is lost or subjected to unauthorised access (both internal and external to the University), modification, disclosure, or other misuse or interference. Examples include:

- unauthorised access to, or the unauthorised collection, use, or disclosure of, UNSW information;
- 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., an 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 or disruption to or denial of IT services resulting in a data breach;
- the loss or theft of a device containing personal information or health information;
- a UNSW database or information repository containing personal information or health information being subject to a cyber-attack;
- a device, database or information repository containing personal information or health information being accessed without authorisation; and/or
- UNSW inadvertently providing personal information or health information to an unauthorised person or entity.

Data breaches involving personal information and/or health information

A data breach involving **personal information** and/or **health information** (whether in digital or hard copy) occurs when there is:

- unauthorised access to or unauthorised disclosure (both internal or external to the University) of, **personal information** or **health information** held by UNSW; or
- there is a loss of **personal information** or **health information** held by UNSW in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

Where a data breach involving personal information or health information occurs, and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, such a data breach will constitute an "**eligible data breach**" and be subject to mandatory data breach notification obligations prescribed by the PPIP Act (and in certain circumstances other privacy laws).

Procedure

1. Identify and report data breaches

1.1 A staff member who has identified a suspected or confirmed a data breach must immediately raise a ticket via the IT Service Centre: (itservicecentre@unsw.edu.au).

1.2 Upon receipt, the IT Service Centre will immediately notify all members of the Data Breach Management Committee (the **Committee)**.

2. Data Breach Management Committee Triage

2.1 Upon the referral of a suspected or confirmed data breach by the IT Service Centre, the Chair of the Committee will:

- immediately update the IT ticket;
- in consultation with the Committee, assign a member of the Data Breach Committee (the lead investigator) to assess and manage the data breach in accordance with the Data Breach Management Plan;
- notify the Critical Incident Response Team if the data breach is determined by the Committee to amount to a major data breach; and
- provide support and guidance to the staff member that identified the data breach.

Privacy data breach

2.2 Where the suspected or confirmed data breach involves personal information or health information, the UNSW Privacy Officer (**Privacy Officer**) will assess the breach. If there are reasonable grounds to suspect that the breach is an **eligible data breach**, the Privacy Officer will:

- immediately update the IT ticket;
- notify the General Counsel of the potential eligible data breach; and
- be appointed as the lead investigator on behalf of the Committee to assess and manage the data breach in accordance with the Data Breach Management Plan, the mandatory data breach notification obligations prescribed by the PPIP Act, and any contractual obligations relating to the data impacted by the breach.

2.3 In accordance with s 59ZJ of the PPIP Act, the functions of the Vice-Chancellor, acting as the head of the University for the purpose of Part 6A of the PPIP Act, are delegated to the General Counsel.

2.4 In accordance with the requirements of the PPIP Act:

a) If the General Counsel is satisfied that an assessment cannot reasonably be conducted within 30 days, they may approve an extension of the period to conduct the assessment. The extension may be approved for an amount of time reasonably required for the assessment to be conducted.

b) If the extension is approved, the General Counsel must, within the 30-day period, request the Privacy Officer to start the assessment; and give written notice to the

Privacy Commissioner that the assessment has commenced and that an extension for the period of the assessment has been approved.

c) If the assessment is not conducted within the extension period, the General Counsel must, before the end of the extension period, give written notice to the Privacy Commissioner that the assessment is ongoing and that a new extension period has been approved.

3. Data Breach Management Plan

3.1 Upon referral of a suspected or confirmed data breach or eligible data breach, the lead investigator will enact the Data Breach Management Plan as follows:

3.2 Immediately contain the breach and conduct a preliminary assessment

3.2.1 The lead investigator will contain the breach and conduct a preliminary assessment.

3.2.2 The breach will be contained by immediately making all reasonable efforts to:

- stop the unauthorised activity; and/or
- recover or limiting the dissemination of records disclosed without authorisation; and/or
- shut down a compromised system.

3.2.3 The following questions will be addressed by the lead investigator in their preliminary assessment:

- Who is affected by the breach?
- What information does the breach involve?
- If the information contains personal information and/or health information, what types of personal information or health information does the breach involve?
- Does the breach amount to a loss of personal information or health information held by UNSW likely result in unauthorised access to, or unauthorised disclosure of, the information?
- Would a reasonable person conclude that the access or disclosure of the personal or health information will likely result in serious harm to an individual to whom the information relates?

3.2.4 In deciding whether the breach would be likely to result in serious harm to an individual to whom the information relates, the lead investigator will consider the following:

- the types of personal information or health information involved;
- the sensitivity of the personal information or health information;
- whether the personal information or health information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused;
- who had access to the personal information or health information;
- whether the person/s who accessed the personal information or health information may have malicious intent and whether they may be able to circumvent security measures; and

- the nature of the harm that has occurred or may occur.

3.3 Evaluate the risks associated with the breach

3.3.1 The lead investigator will assess the risks associated with the breach by considering the following questions:

- What was the cause of the breach?
- What is the extent of the breach?
- Is there a risk of ongoing breaches or further exposure of the information?
- Is there evidence of theft?
- Is this a systemic problem within UNSW or an isolated incident?
- How many people are affected by the breach?
- What other harms could result from the breach?
- Have there been other breaches that could have a cumulative effect?
- How could the information be used?
- Has the information been recovered?
- What steps have already been taken to mitigate the harm?
- Is there a reputational risk to UNSW?
- Is there a commercial or intellectual property risk for UNSW?

3.3.2 if there are reasonable grounds to suspect, or there is evidence to conclude, that an eligible data breach or a data breach has occurred, the lead investigator will immediately report their conclusion to the General Counsel and the Data Breach Management Committee.

3.4. Notifications to affected individuals or entities

3.4.1 Where the Privacy Officer concludes or has reasonable grounds to suspect that the breach amounts to an eligible data breach and the General Counsel agrees with this assessment, the General Counsel will:

- immediately notify the Privacy Commissioner of the eligible data breach using the approved form published by the Privacy Commissioner, unless it is not reasonably practicable for the information to be provided; and
- as soon as reasonably practicable, notify each individual to whom the personal information the subject of the breach relates, or each affected individual or their authorised representative, in writing about the breach, unless exempt from doing so.

3.4.2 The notification to each individual will provide affected individuals with an accurate description of what happened, what risks may arise and what they can do to protect themselves. The notification will specifically contain the following information:

- the date the breach occurred;
- a description of the breach;
- how the breach occurred;
- the type of breach that occurred;

- the personal information that was the subject of the breach;
- the amount of time the information was disclosed for
- actions UNSW has taken or plans to ensure the personal information is secure;
- actions UNSW has taken to control or mitigate the harm done to the individual;
- recommendations about the steps the individual should consider taking in response to the eligible data breach; and
- information about:
    - how to make a privacy-related complaint to the Privacy Commissioner;
    - how to seek an internal review of UNSW's conduct; and
    - the contact details for UNSW or a person nominated by UNSW for the individual to contact about the breach.

3.4.3 If it is not reasonably practicable to directly notify any or all the individuals affected by the breach, the General Counsel will:

- arrange to have published a public notification on UNSW's website for at least 12 months detailing information about the breach, such as: the date the breach occurred, how the breach occurred, the type of breach that occurred, the amount of time the information was disclosed, actions taken or planned to ensure the personal information is secure, where to contact for assistance or information;
- take reasonable steps to publicise that notification; and
- provide the Privacy Commissioner with information about how to access the public notification on UNSW's website.

3.4.4 In addition, the Committee, consulting with relevant officers of the University as required, will determine if it is appropriate and necessary to notify other third parties, such as:

- 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 that is lost/stolen such as State Records NSW or Museums of History NSW.

3.5 Notification to staff member that reported the breach

3.5.1 The Chair of the Data Breach Management Committee will notify the staff member that reported the breach of the outcome of the data breach and assist them in responding to any requests for information in relation to the breach from stakeholders or other third parties.

3.6 Prevention of future breaches

3.6.1 Once immediate steps have been taken to mitigate the risks associated with a breach, and relevant notifications have been made, the lead investigator will:

- investigate the cause of the breach
- conduct a post-breach review and evaluation on the root cause of the breach
- in consultation with the General Counsel, identify if there is a risk of legal proceedings against the University as a result of the breach (e.g. class action by affected individuals) and will provide a report to the Committee.

3.6.2 The Chair of the Committee will:

- on behalf of the Committee, provide a brief to the UNSW Safety & Risk Committee of Council on the outcome of the post-breach review and relevant recommendations; and
- publish information about the data breach, the steps UNSW took to mitigate the harm done by the breach and the actions to prevent future breaches in UNSW's internal Data Breach Incident Register.

4. Roles and Responsibilities

Role	Responsibility
UNSW Staff	Identifies and reports a suspected or confirmed data breach or eligible data breach. Implements measures to ensure UNSW data is protected.
Data Breach Management Committee *	Implements the Data Breach Management Plan for suspected or confirmed data breach or eligible data breach, appoints lead investigator, notifies General Counsel of suspected or confirmed eligible data breach
Lead Investigator	Investigates the suspected or confirmed data breach or eligible data breach
IT Service Centre	Reports any communications regarding data breach or eligible data breach to the Data Breach Management Committee.
General Counsel	Notifies the NSW Privacy Commissioner and affected individuals in the case of an eligible data breach

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

- Chief Data & Insights Officer (UNSW Planning & Performance)
- Director Cyber Security (UNSW IT, Chief Information Security Officer)
- Head of Compliance and Controlled Entities Law (Legal)
- Privacy Officer (Legal)
- Director, Customer Services Delivery (UNSW IT)

- Director of Risk (Division of Planning & Assurance)
- Manager, Records and Archives

Accountabilities	
Responsible Officer	Provost
Contact Officer	Chief Data & Insights Officer
Supporting Information	
Legislative Compliance	This policy supports the University's compliance with the following legislation: *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) (NSW Legislation website) *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) (NSW Legislation website) *Privacy Act 1988 (*Cth) *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 Regulation 2014 (2014-549) (NSW) (PPIP Regulation)
Supporting Documents	Privacy Policy Privacy Management Plan
Related Documents	IPC Data Breach Guidance Data Classification Standard Data Governance Policy Data Handling Guidelines IT Security Policy IT Security Standards Recordkeeping Policy Recordkeeping Standard
Superseded Documents	Data Breach Policy v1.2 Data Breach Procedure v1.0
File Number	2018/07574

Definitions and Acronyms	
Cyber Breach	A cyber breach is a breach of data that results in a cyber security incident.
Cyber Security Incident	A cyber security incident is a cyber security event that has been assessed (in accordance with the Cyber Security Standards) to have a potential adverse impact on the confidentiality, integrity, or availability of an UNSW Information Resource".
Data Breach	A data breach occurs when l information (including personal or health 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 or health 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 to contain and remediate the data breach
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.
Eligible Data Breach	An eligible data breach means '(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or (b) personal information held by a public sector agency is lost in circumstances where (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and (ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.'
Health Information	Information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Health Privacy Principles	The obligations prescribed by the *Health Records and Information Privacy Act 2002* (NSW) by which the University must abide when it collects, stores, uses or discloses health information.
Information Protection Principles	The obligations prescribed by the *Privacy and Personal Information Protection Act 1998* (NSW) by which the University must abide when it collects, stores, uses or discloses personal information.
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.
Privacy Commissioner	Means the NSW Privacy Commissioner appointed under the *Privacy and Personal Information Protection Act 1998* (NSW).
Serious Harm	Serious harm can include 'physical, financial, or material harm, emotional or psychological harm or reputational harm. The impact of the harm can vary from person to person, but may include: • financial loss through fraud • a likely risk of physical or psychological harm, such as by an abusive ex-partner • identity theft, which can affect your finances and/or credit record • serious harm to an individual's reputation.'

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
1.1	Director of Governance	21 May 2018	21 May 2018	Added IPC Data Breach Guidance to the Related Documents section
1.2	Director of Governance	12 June 2019	12 June 2019	Administrative update: Section 5 and Responsible Officer
2.0	Vice-Chancellor and President	3 November 2023	3 November 2023	Full review addressing amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). Consolidation of Data Breach Policy and Data Breach Procedure into one policy.