Data Breach Policy and Procedure

Version

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 occursUSoccursUSly to

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

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 wim0 g0osed wim0us

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

4. Roles and Responsibilities

Role	Responsibility

Director of Risk (Division of Planning & Assurance)

Manager, Records and Archives

Accountabilities	
Responsible Officer	Provost
Contact Officer	Chief Data & Insights Officer
Supporting Information	

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
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 s wh wh wh wh wh wh w wh w 625.42

Health Privacy Principles