DATA BREACH POLICY 2023

The Vice-Chancellor and President adopts the following policy, as delegate of the Senate of the University of Sydney.

Dated: 19 December 2023

Last amended:

Position: Professor Mark Scott

CONTENTS

1 Name of policy 1
2 Commencement 1
3 Statement of intent 2
4 Application 2
5 Definitions 2
6 Data breach 5
7 Eligible data breach 5
8 Preventing a data breach 6
9 Responding to a data breach 7
10 Step 1. Report the breach 7
11 Step 2. Contain and mitigate 7
12 Step 3. Assess and investigate 8
13 Step 4. Notify 10
14 Step 5. Review 11
15 Roles and responsibilities 12

Notes 14

Amendment history 14

1 Name of policy

This is the Data Breach Policy 2023.

2 Commencement

This policy commences on 19 December 2023.

3 Statement of intent

This policy:

(a) complies with the requirements of the *Privacy and Personal Information Protection Act 1998* (NSW);

(b) establishes the mandatory notification of data breach scheme (MNDB);

(c) establishes strategies for containing, assessing and reporting data breaches, including for eligible data breaches; and

(d) establishes roles and responsibilities for managing data breaches.

4 Application

This policy applies to:

(a) staff, students and affiliates; and

(b) data breaches, including eligible data breaches.

5 Definitions

assessment	means evaluating whether the data breach is an eligible data breach. The assessment must be completed within 30 days. **Note**: See ss 59H and 59E(2)(b) of the *Privacy and Personal Information Protection Act 1998* (NSW).
assessor	means a person appointed to carry out an assessment under clause 12. An assessor may be: • employed internally by the University; or • employed by an external party. **Note**: See s 59G(2) of the *Privacy and Personal Information Protection Act 1998* (NSW).
cyber security	means the team within the Information and Communications Technology unit that is responsible for protecting the University's data and technology.
data breach	has the meaning given in clause 6 of this policy.

eligible data breach	has the meaning given in s 59D of the *Privacy and Personal Information Protection Act 1998* (NSW). At the date of this policy this is: • unauthorised access to, or unauthorised disclosure of, personal information held by the University; which • a reasonable person would conclude would be likely to result in serious harm to an individual to whom the information relates. **Note**: Section 26WE of the *Privacy Act 1988* (Cth) has the same definition. See clause 13(5) of this policy for when to notify the Commonwealth Information Commissioner.
eligible data breach incident register	has the meaning given in s 59ZE of the *Privacy and Personal Information Protection Act 1998* (NSW) and subclause 8(2) of this policy.
external party	means any party external to the University with whom the University enters into an agreement to supply specific skills, services or consultancy arrangements.
health information	has the same meaning in s 6 of the *Health Records and Information Privacy Act 2002* (NSW). This includes: • information about an individual's physical or mental health or, disability; • blood or DNA samples; • information about a health service provided to an individual; • information or opinions about an individual's physical or mental health, or disability.
ICT	means information and communications technology within any University organisational unit.
Mandatory Notification of Data Breach (MNDB) scheme	means the scheme specified in Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW). This scheme requires the University to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm. **Note**: See clause 13(5) for when to notify the Commonwealth Information Commissioner under the *Privacy Act 1988* (Cth).
OGC	means the Office of General Counsel.

organisational resilience	has the meaning given in the *Risk Management Policy 2017*, which at the date of this policy is: means the ability to adapt to changing conditions. It includes the ability to respond to, and recover from, disruptions and the ability to change in order to prosper from adversity. This includes, but is not limited to, managing: • emergency responses; • crises; • business continuity; • ICT disaster recovery; • cyber security breaches; • financial shock event recovery; and • all other plans and activities designed to enable the University to respond to emerging risks that may impact its ongoing viability.
organisational unit	means any of the following: • faculty; • University school; • a portfolio or professional services unit controlled by a Principal Officer; • a level 4 centre, as described in the *Centres and Collaborative Networks Policy 2017.*
personal information	has the meaning given in s 4 in of the *Privacy and Personal Information Protection Act 1998* (NSW).
PPIPA	means the *Privacy and Personal Information Protection Act 1998* (NSW).
Privacy Commissioner	means the Commissioner at the Information and Privacy Commission. This agency administers NSW legislation dealing with data breaches that are likely to cause serious harm.
public notification register	has the meaning given in s 59P of the *Privacy and Personal Information Protection Act 1998* (NSW) and subclause 13(6) of this policy.
researcher	has the same meaning given in the *Research Code of Conduct 2023*, which at the date of this policy is: means any staff member, student or affiliate (including professors emeriti) who conducts or assists with the conduct of research (including research trainees).

serious harm means harm that has a substantial detrimental effect on the individual. It includes:

- physical harm;
- economic, financial or material harm;
- emotional or psychological harm;
- reputational harm; and
- other forms of serious harm that a reasonable person would identify as a possible outcome of the data breach.

Note: The effect on the individual must be more than mere irritation, annoyance or inconvenience.

6 Data breach

(1) A data breach occurs when personal or health information held by the University has been:

(a) unlawfully accessed;

(b) improperly shared;

(c) lost;

(d) accidentally or unlawfully destroyed; or

(e) deliberately altered with intent to misrepresent or deceive.

(2) Data may be lawfully altered:

(a) in ways that do not contravene this policy;

(b) to de-identify it; or

(c) in the case of research data, as a requirement of human research ethics committee approval.

7 Eligible data breach

(1) An eligible data breach is one where a reasonable person would conclude that disclosure of the information is likely to result in serious harm to an individual to whom the information relates.

(2) The University Archivist and Manager, Privacy Compliance must establish and maintain an eligible data breach incident register.

(3) The register is located within the corporate recordkeeping system.

(4) For each incident the register should record:

(a) who was notified of the breach;

(b) date of the breach;

(c) the type of breach (unauthorised disclosure, unauthorised access or loss of information);

(d) the sensitivity of data involved in the breach;

(e) the estimated number of records affected by the breach;

(f) steps taken to mitigate harm done;

(g) actions taken to prevent future breaches; and

(h) the estimated cost of the breach.

8 Preventing a data breach

(1) The University will take all reasonable steps to prevent a data breach.

(2) The Chief Information Security Officer will:

(a) implement technical controls to protect data and technology;

(b) monitor for suspicious activity that may pose a threat to the University; and

(c) regularly assess the University's cyber security risk management and treatment plan.

(3) The Chief Information Officer will:

(a) provide mechanisms for storing personal and health information in a secure manner; and

(b) maintain strong ICT governance controls, including security and privacy features in ICT projects.

(4) The University Archivist and Manager, Privacy Compliance will:

(a) regularly review the eligible data breach incident register and actions recorded to prevent future breaches;

(b) undertake privacy risk assessments for all necessary systems, projects and processes;

(c) provide privacy advice and guidance to organisational units; and

(d) support organisational units to consider privacy in system and process development.

(5) Human resources will provide training about:

(a) identifying personal and health information;

(b) identifying, responding to and managing data breaches;

(c) understanding privacy and cyber principles and current threat trends.

(6) Researchers will:

(a) comply with data sharing agreements;

(b) store data securely and retain it consistently with legal and contractual data retention obligations; and

(c) obtain all appropriate ethics approvals and avoid collecting, using, reusing or sharing of data without proper ethics approval.

(7) Staff will update relevant policies and procedures on a regular basis.

(8) Organisational units and system owners will implement appropriate controls and work practices to protect personal information and minimise the risk of data breaches.

(9) Staff, students and affiliates will take all reasonable steps to prevent data breaches by following safe practices and complying with policy and procedures.

Note: See *Cyber Security Policy 2019*; *Cyber Security Procedures 2019*; *Technical Standards*; *Acceptable Use of ICT Resources Policy 2019; Research Data Management Policy 2014; Privacy Policy 2017; Privacy Procedures 2023; Research Code of Conduct 2023.*

(10) Procurement and sourcing processes must request any external party providing services to the University to manage any data breach consistently with this policy.

Note: Relationships with external parties are usually covered by legally binding contracts. Contact the OGC for advice.

9 Responding to a data breach

(1) The University will respond to a data breach with the steps specified in clauses 10-14.

(2) The University Archivist and Manager, Privacy Compliance will, if required, ask an internal organisational unit or an external party to manage a data breach consistently with this policy.

(3) All relevant organisational units and researchers must support the data breach response process.

10 Step 1. Report the breach

(1) Staff, students and affiliates who become aware of a data breach must immediately report the breach to:

(a) privacy.enquiries@sydney.edu.au;

(b) the University's ICT Helpdesk by telephone (02) 9351 2000; or

(c) the Privacy team by using the reporting form on the intranet's Privacy page.

(2) The following information should be included in any report:

(a) details of the breach;

(b) the suspected breach cause;

(c) the date of the breach;

(d) the data that was disclosed or accessed;

(e) the data location; and

(f) any other relevant information.

11 Step 2. Contain and mitigate

(1) The University Archivist and Manager, Privacy Compliance will take immediate action to:

(a) contain the breach; and

(b) reduce its impact.

(2) If necessary, the University Archivist and Manager, Privacy Compliance will limit access to, or distribution of, the personal information by consulting with:

(a) the Chief Information Officer;

(b) the Chief Information Security Officer; or

(c) any other relevant internal or external party.

12 Step 3. Assess and investigate

(1) The University Archivist and Manager, Privacy Compliance will:

(a) conduct an initial assessment of the breach; or

(b) appoint an assessor to do so.

(2) The purpose of the initial assessment is to:

(a) identify the nature and extent of the breach;

(b) preserve any evidence necessary to investigate it; and

(c) if relevant, inform any external party involved.

(3) If there is reasonable suspicion that the breach will result in serious harm to affected individuals, the assessor will conduct a full assessment and consider:

(a) the types of personal information involved in the breach;

(b) the sensitivity of the personal information involved in the breach;

(c) whether the personal information is or was protected by security measures;

(d) how those involved in the breach obtained access to the information;

(e) whether access was intended:

(i) to cause harm; or

(ii) to circumvent the security measures protecting the information;

(f) the risk posed by the breach; and

(g) whether the access to, or disclosure of, the information is likely to result in serious harm to an individual to whom the personal information relates.

Note: See the Commissioner's Guidelines on the assessment of data breaches.

(4) In assessing the risk, the assessor will review the circumstances of the breach and classify the incident as low, medium or high risk.

(a) An incident is **low risk** where:

(i) individual data is lost or exposed; and

(ii) it is unlikely that real harm could occur.

(iii) An example is paper files that have been accidentally left in a meeting room and are promptly collected.

(b) An incident is **medium risk** where:

(i) personal information is lost or exposed;

(ii) there is no evidence of malicious intent by any external party who may access the information; and

(iii) the data is somewhat protected, e.g. a password is required to open the document.

(iv) An example is an email message containing a document with personal information that is accidentally sent to the wrong person.

(c) An incident is **high risk** where:

(i) personal information is lost or exposed; and

(ii) the loss or exposure is likely to result in serious harm to individuals.

(iii) An example is where an external hacker has broken the University's firewall to obtain personal information.

(iv) A high risk data breach will generally be an eligible data breach.

Note: The risk classifications are guidelines only. Any data breach could potentially be an eligible data breach.

(5) Where the assessor has classified an incident as high risk, the University Archivist and Manager, Privacy Compliance may recommend that an ad hoc organisational resilience committee, such as an Emergency Response Team under the Organisational Resilience Framework, is convened to coordinate the breach response.

Note: See the *Risk Management Policy 2017* for more information about resilience committees and the Organisational Resilience Framework.

(6) The assessor will consider advice from relevant stakeholders, e.g. the Chief Information Officer, Chief Information Security Officer, General Counsel or head of an organisational unit, who may contribute to the full assessment to either:

(a) complete an assessment of the data breach within 30 calendar days; or

(b) seek an extension from the University Archivist and Manager, Privacy Compliance.

(7) The assessor will provide a copy of the assessment report to:

(a) the Vice-Chancellor;

(b) the General Counsel; and

(c) if relevant:

(i) the University Archivist and Manager, Privacy Compliance; and

(ii) an Emergency Response Team.

Note: See the Organisational Resilience Framework.

(8) The assessment report must include:

(a) the outcome of the assessment;

(b) in their view, whether the data breach is an eligible data breach and has, or will, result in serious harm;

(c) action taken to contain and manage the breach; and

(d) a mitigation plan to:

(i) reduce the impact of the breach;

(ii) prevent further occurrences; and

(iii) reduce the harm done;

and

(e) notifications to affected individuals.

(9) A copy of the report must be recorded in the University's recordkeeping system.

Note: See *Recordkeeping Policy 2017*.

(10) The University Archivist and Manager, Privacy Compliance will consider the report and decide if there has been an eligible data breach.

13 Step 4. Notify

(1) If there has been an eligible data breach, the University Archivist and Manager, Privacy Compliance must notify the Privacy Commissioner of the breach in the approved form.

(2) The Privacy team will support relevant organisational units to support notifying individuals, or organisations affected by the breach, unless an exemption applies.

(3) For eligible data breaches, the General Counsel, together with the University Archivist and Manager, Privacy Compliance, will determine whether the University is exempt from the requirement to notify. The six exemptions are:

(a) if the breach involves multiple agencies;

Note: See section 59S of PPIPA.

(b) if there are ongoing investigations or legal proceedings;

Note: See section 59T of PPIPA.

(c) if the University has taken action to prevent the breach resulting in serious harm to an individual;

Note: See section 59U of PPIPA

(d) if the notification would result in disclosing secret information that is governed by a legal provision restricting its release;

Note: See section 59V of PPIPA

(e) if the notification is likely to cause serious harm to the health and safety of an individual;

Note: See s59W of the PPIPA and Commissioner's assessment guidelines.

(f) if the University believes notifying the individual will worsen cyber security, or lead to further data breaches.

Note: See section 59X of PPIPA

(4) The University Archivist and Manager, Privacy Compliance together with the General Counsel and Chief Information Security Officer will decide whether others should be notified, including:

(a) law enforcement agencies; or

(b) national or international privacy or cyber security regulators.

(5) The Commonwealth Information Commissioner must be notified if the data breach involves:

(a) a tax file number;

(b) a Medicare number; or

(c) research governed by a University funding agreement which requires compliance with the *Privacy Act 1988* (Cth).

Note: See the Notifiable Data Breaches scheme managed by the Office of the Australian Information Commissioner.

(6) If the University is unable to notify affected individuals, the University Archivist and Manager, Privacy Compliance will publish a public notification register on the University website.

(7) For each eligible data breach, the public notification register will include:

(a) the date the breach occurred;

(b) a description of the breach;

(c) how the breach occurred;

(d) the type of breach;

(e) the personal information that was the subject of the breach;

(f) who to contact about the breach;

(g) the amount of time the personal information was disclosed;

(h) actions taken, or planned, to:

(i) ensure the personal information is secure; or

(ii) control or mitigate the harm done to the individual;

(i) recommendations about the steps the individual should take in response to the eligible data breach; and

(j) how to make a complaint under PPIPA.

(8) The public notification register will not include:

(a) personal or health information; or

(b) any information compromising the University's functions.

(9) The University Archivist and Manager, Privacy Compliance will:

(a) inform the Commissioner about how to access the register; and

(b) keep information about the eligible data breach on the University website for at least 12 months after its first publication.

Note: See section 59P of PPIPA.

14 Step 5. Review

(1) The University Archivist and Manager, Privacy Compliance, together with other relevant stakeholders, e.g. the General Counsel, ICT or Cyber Security and affected organisational units, will:

(a) investigate the data breach to identify all relevant causes;

(b) recommend actions to prevent any reoccurrence.

(2) Actions to prevent reoccurrence may include:

(a) reviewing the University's ICT systems to determine whether they are able to withstand potential security threats;

(b) undertaking a security audit of the physical and technical security controls that protect the University's assets, information, and facilities;

(c) reviewing and updating the University's data breach training program to create a security-aware culture and prevent security incidents;

(d) reviewing arrangements with external service providers to verify they have adequate security measures in place to prevent any potential security breaches that could affect the University; or

(e) amending business processes or systems.

15 Roles and responsibilities

(1) The **Vice-Chancellor** is responsible for:

(a) fostering a workplace culture that promotes the protection of data and technology;

(b) overseeing the allocation of resources to enable effective compliance with PPIPA;

(c) publishing a data breach policy.

(2) The **General Counsel** is responsible for:

(a) deciding whether the University is exempt from the requirement to notify an affected individual;

(b) deciding whether national or international privacy or cyber security regulators or law enforcements agencies should be notified about a data breach.

(3) The **University Archivist and Manager, Privacy Compliance** is responsible for:

(a) regularly reviewing the eligible data breach incident register and actions recorded to prevent future breaches;

(b) undertaking privacy risk assessments for all necessary systems, projects and processes;

(c) providing privacy advice and guidance to organisational units;

(d) supporting organisational units to implement privacy features in system and process development;

(e) assessing a data breach or appointing an assessor to conduct an assessment of the data breach;

(f) if the breach is an eligible data breach, notifying the Commissioner;

(g) establishing and maintaining an eligible data breach incident register;

(h) if required, establishing and maintaining a public notification register and notifying the Commissioner about access;

(i) supporting the relevant organisational unit, researchers and staff to notify individuals or organisations affected by the breach, including external parties;

(j) maintaining a notification about the eligible data breach on the University website for at least 12 months after its first publication Assessor;

(k) regularly reviewing the eligible data breach incident register and actions recorded to prevent future breaches;

(l) investigating each data breach to determine all relevant causes; and

(m) considering relevant measures to implement to prevent any breach reoccurrence.

(4) An **assessor** is responsible for:

(a) conducting a preliminary fact-finding about the breach to immediately mitigate harm posed by the breach;

(b) conducting a full assessment of the breach;

(c) determining whether personal or health information has been accessed or disclosed because of the breach;

(d) assessing whether a reasonable person would conclude that the data breach would be likely to result in serious harm to affected individuals; and

(e) determining whether an eligible data breach has occurred.

(5) **The Chief Information Security Officer** is responsible for:

(a) implementing technical controls to protect data, such as data loss prevention tools;

(b) monitoring for suspicious activity that may pose a threat to the University;

(c) mitigating the risk of a breach by regularly assessing the University's cyber security risk management and treatment plan by:

(i) implementing measures to limit access to, or distribute, the personal information;

(ii) investigating the data breach to determine all relevant causes;

(iii) preventing further access to, or distribution of, the information;

(d) supporting data breach assessments and any necessary remediations.

(6) **The Chief Information Officer is** responsible for:

(a) providing mechanisms for storing personal and health information in a secure manner;

(b) maintaining strong ICT governance controls, including security and privacy by design, in ICT projects;

(c) supporting data breach assessments and any necessary remediations.

(7) **Human Resources** are responsible for providing mandatory training to assist staff and affiliates to:

(a) identify personal and health information;

(b) respond to and manage data breaches;

(c) comply with privacy and cyber principles; and

(d) understand current threat trends.

(8) **Organisational units** and researchers are responsible for:

(a) implementing safe work practices and systems to minimise the risk of data breaches;

(b) supporting data breach assessments and any necessary remediations.

(9) **Staff, students and affiliates** are responsible for:

(a) complying with relevant policy and procedures;

(b) taking all reasonable steps to keep data safe; and

(c) reporting a data breach.

NOTES

Data Breach Policy 2023

Date adopted:	19 December 2023
Date commenced:	19 December 2023
Administrator:	University Archivist and Manager, Privacy Compliance
Review date:	19 December 2028
Rescinded documents:	none
Related documents:	*Privacy Act 1988* (Cth)
	Privacy and Personal Information Protection Act 1998 (NSW)
	Health Records and Information Privacy Act 2002 (NSW)
	Centres and Collaborative Networks Policy 2017
	Cyber Security Policy 2019
	Cyber Security Procedures 2019
	Acceptable Use of ICT Resources Policy 2019
	Research Data Management Policy 2014
	Privacy Policy 2017
	Privacy Procedures 2023
	Research Code of Conduct 2023
	Risk Management Policy 2017
	Technical Standards

AMENDMENT HISTORY

Provision	Amendment	Commencing