Data Breach Policy

Section 1 - Purpose

(1) This Policy establishes the principles for reporting and responding to a data breach and an eligible data breach. The Policy identifies roles and responsibilities, the mechanisms in place to prevent data breaches from occurring and the University's reporting and notification requirements if an eligible data breach has occurred. The Policy aims to assist the University in avoiding or minimising harm to affected individuals as a result of data breaches.

(2) This Policy has been developed in line with the Privacy and Personal Information Protection Act 1998 (NSW)(PPIP Act) and the guidance from the Information and Privacy Commission New South Wales.

Background

(3) The University must comply with the PPIP Act and the Health Records and information Privacy Act 2002 (NSW)(HRIP Act)in respect of Personal and Health Information it collects and uses.

(4) Through the introduction of a Mandatory Notification of Data Breach Scheme (MNDB Scheme),the PPIP Act requires the University to notify the Information and Privacy Commission New South Wales and affected individuals of data breaches involving Personal Information that are likely to result in serious harm.

(5) Personal Information for the purposes of the MNDB Scheme includes information about an individual's physical or mental health, disability and information connected to the provision of a health service.

(6) The University's Controlled Entities which are considered organisations within the meaning of the Privacy Act 1998 (Cth) must comply with the Notifiable Data Breaches (NDB) scheme governed by the Australian Information Commissioner. The requirements of the MNDB scheme are broadly aligned with the NDB scheme.

Scope

(7) This Policy applies to:

a. all Staff and Affiliates of the University and its Controlled Entities;
b. all Students of the University, including former Students;
c. all University researchers; and
d. any person who handles Personal or Health Information for or on behalf of the University or its Controlled Entities, including contractors, agents, visitors, honorary, clinical or adjunct appointees and consultants of the University.

Section 2 - Policy

Principles

(8) The University is committed to effective management and governance of its data and information and the privacy rights of its Students, Staff and Affiliates, and third parties.

(9) The University implements a range of activities and controls to ensure the security of data and information and that privacy obligations are met, including staff training, guidance, and policy review/development.

(10) The University will ensure there are security safeguards in place, as are reasonable in the circumstances, to protect Personal Information held by the University against loss, unauthorised access, use, modification or disclosure, and any other misuse.

(11) All Staff, Students, and Affiliates of the University have a responsibility to report actual or suspected data breaches in a timely manner.

(12) The University recognises the value and importance of responding to suspected or actual data breaches quickly and efficiently.

(13) The University will take all reasonable and necessary steps to contain data breaches and minimise the harm to affected individuals.

Data Breach

(14) A data breach occurs when information held by the University is subject to unauthorised access, disclosure, or is lost in circumstances where the loss is likely to result in unauthorised access or disclosure.

(15) A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. Examples of data breaches include:

a. malicious users sending phishing emails to access information or trick a user into performing a particular action;
b. having vulnerable IT systems that have weaknesses that can be impacted by common exploit tools and techniques available on the internet;
c. leaving access to sensitive data open when it should be restricted to only a few users;
d. inadvertent disclosure of Personal Information due to human error; or
e. loss or theft of a University issued laptop.

Eligible Data Breach

(16) The MNDB Scheme applies where an ‘eligible data breach’ has occurred.

(17) An eligible data breach occurs when:

a. there is unauthorised access to, or unauthorised disclosure of, Personal Information held by the University 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 the University is lost in the 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.

(18) Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual, which is more than irritation, annoyance or inconvenience. Harm may include 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 for the data breach.

(19) An eligible data breach can occur within the University, between the University and another public sector agency,

or by an external person or entity accessing data held by the University without authorisation.

Section 3 - Procedures

Responding to a Data Breach

(20) The University will undertake a systematic approach to managing any data breach, which includes the key activities outlined in this Procedure.

Reporting

(21) A data breach or suspected data breach can be reported through several means, including but not limited to:

a. a cyber security breach reported through the Cyber Security Incident Response;
b. a Staff member, Student or Affiliate identifying a data breach by notifying the IT Service Desk; or
c. an external party to the University raising concerns about Personal Information being compromised.

(22) All University Staff, Students and Affiliates are responsible for identifying a data breach or suspected data breach and promptly reporting it to either the:

a. IT Service Desk;
b. Privacy Officer;
c. Chief Information Security Officer; or
d. the Staff member's manager/supervisor.

Validation

(23) The Cyber Security Team will validate any identified data breach or suspected data breach and confirm whether data and/or Personal Information has been compromised.

Restriction/Containment

(24) When a data breach has been confirmed, the Cyber Security Team will immediately make all reasonable efforts to perform restrictive and containment activities to ensure that no further breaches can occur. The containment measures will depend on the nature of the breach and can involve changing IT controls, physical controls, process-oriented controls, and any other containment measures such as shutting down, suspending, or isolating systems or disabling compromised accounts, that restrict the incident from further impacting the University.

Assessment

(25) Once the data breach has been validated and restricted/contained, the Privacy Officer, in consultation with relevant University officers, will determine whether there are reasonable grounds to suspect there may have been an eligible data breach and if confirmed, will refer this to the Vice-Chancellor for the appointment of an Assessor.

(26) The Vice-Chancellor will appoint a Staff member or external party not involved in an action or omission that led to the eligible data breach (Assessor) to conduct an assessment of an identified potential data breach to understand the risk of harm to affected individuals. The University will take all appropriate steps to limit the impact of a data breach. If requested, the Assessor must provide information and updates to the Privacy Officer about the assessment.

(27) As soon as possible but no later than 30 days of becoming aware of a data breach, the Assessor will carry out an assessment of whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach.

(28) The Assessor may engage necessary advisors and expertise as required.

(29) The key considerations for assessment include the types and sensitivity of Personal Information involved in the breach and the nature of the harm that has occurred or may occur. A non-exhaustive list of factors that may be considered when assessing a data breach include:

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. the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given;
e. the likelihood the persons specified in paragraph(d):
    i. have or had the intention of causing harm; or
    ii. could or did circumvent security measures protecting the information;
f. the nature of the harm that has occurred or may occur; and/or
g. other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

(30) If an assessment cannot reasonably be conducted within 30 days, the Assessor will propose an extension period to the Vice-Chancellor, who will determine and approve the additional amount of time reasonably required to conduct the assessment.

(31) If an extension period is approved, the Vice-Chancellor, or a person with delegated authority, will give written notice of this to the Privacy Commissioner.

(32) If the eligible data breach is considered a critical incident under the Incident Management Policy, the Assessor (if requested) must provide updates and information to the Critical Incident Management Team.

(33) Each data breach will be assessed on an individual basis.

Communications

(34) The Privacy Officer must notify the Privacy Commissioner immediately of an eligible data breach.

(35) Unless an exemption applies, the Privacy Officer, in consultation with relevant University officers, will take reasonable steps to notify:

a. each individual to whom the Personal Information the subject of the breach relates; or
b. each affected individual; or
c. issue a public notification of the eligible data breach if individual notification is not reasonably practicable.

(36) The method of notification will be determined on a case-by-case basis and may include communication through Student or Staff email accounts or telephone.

(37) The Privacy Officer, in consultation with the relevant officers of the University, will also determine whether notification to other third parties is necessary. Depending on the nature of the eligible data breach, this may include the police, insurance providers, financial institutions, or external agencies impacted by the eligible data breach.

(38) The Privacy Officer will develop a data breach communications strategy to identify roles and responsibilities in the event of an eligible data breach. The strategy will outline responsibilities for communications, establish the expected timeframes for notification and a template for communications to notify required individuals.

Root Cause Eradication and Return to Normal Operations

(39) After the data breach has been restricted/contained, the Cyber Security Team will ensure that the root cause of the issue has been addressed, to also prevent subsequent compromises. This may involve making permanent changes to a system, process, or physical property to ensure the original weakness no longer exists.

(40) The Cyber Security Team will take measures to return to normal operations which may involve removing the special containment measures with confidence that the root cause of the weakness no longer exists.

Post Breach Review and Evaluation

(41) The Cyber Security Team will conduct a post breach review and consider what improvements can be made to processes, systems, or controls on an ongoing basis to prevent the data breach from reoccurring.

(42) The review and evaluation report will be provided to the Chief Information Security Officer for consideration and submitted to the Chief Information and Digital Officer, prior to recommendation to relevant stakeholders. The report may include recommendations such as:

a. updating relevant response plans;
b. conducting audits to ensure any preventative measures that were implemented are operating effectively;
c. considering changes to policies and procedures; and
d. revising or introducing staff training practices.

Record Keeping

(43) The University publishes a notification register on its Privacy webpage, maintained by the Privacy Officer, which lists any eligible data breaches that required notification to the Privacy Commissioner and public notification to impacted individuals, where relevant.

(44) The University also maintains an internal register of data breaches, including eligible data breaches, which is updated by the Chief Information Security Officer and the Privacy Officer.

(45) The University will retain records relating to data breaches, including eligible data breaches, in line with the Records and Information Management Policy.

Preventative Measures

(46) The University has the following preventative measures in place to prepare for a data breach:

a. a broader Data Governance Framework encompassing the Cyber Security Policy, Information Classification and Handling Procedure, Records and Information Management Policy, the Computer and Network Security Policy and the Privacy Policy;
b. compulsory Cyber Security training to assist Staff in preventing cyber attacks and avoiding security breaches. The training provides practical ways to ensure safe working online and how to identify and report cyber security incidents; and
c. when the University engages external service providers, the University will ensure that there are privacy obligations on the external service provider concerning any Personal or Health Information they receive or have access to during the term of the contract. Contracted service providers performing tasks that involve Personal Information must have appropriate data breach clauses in agreements where (at a minimum):
    i. they will comply with all applicable state and federal privacy legislation and mandatory codes in relation to any Personal or Health Information;
    ii. there are limitations on the use of data only for specified purposes;

iii. there is a data breach response plan that includes timeframes for reporting suspected breaches and a straightforward process for reporting a data breach and cooperating in responding to a breach; and
iv. there are provisions around the disposal of data upon contract termination.

The University's agreement templates are reviewed and updated on a regular basis to ensure regulatory changes are addressed.

Roles and Key Responsibilities

(47) All Staff, Students and Affiliates of the University are responsible for:

a. recognising a data breach incident and promptly reporting it to the IT service desk, Privacy Officer, Cyber Security or their manager/supervisor;
b. only collecting or creating information required for the designated purpose in accordance with the University's Privacy Policy;
c. only retaining information for the length of time that is necessary for the designated purpose; and
d. restricting access to information to only those who require it.

(48) The Chief Information Security Officer is responsible for:

a. ensuring that the Cyber Security Team validate and rate cyber security incidents, including data breaches, as they occur;
b. notifying the Privacy Officer where an incident may involve Personal Information;
c. considering whether to inform the Chief Risk Officer under the Incident Management Policy, where appropriate;
d. performing the appropriate and necessary containment measures, root cause eradication and post breach review;
e. reviewing, testing and updating this Policy on an annual basis to ensure it is accurate and aligned to related policies and procedures; and
f. providing guidance and training to Staff on best practice for cyber security and data breaches.

(49) The IT Service Desk is responsible for:

a. collating reports from Staff, Students and Affiliates, creating a case and tracking an IT incident as it progresses, including initial reports of data breaches; and
b. informing the appropriate contact within the University of the data breach including Information Security and the Privacy Officer, where relevant.

(50) The Privacy Officer is responsible for:

a. assessment of data breaches that involve Personal Information;
b. coordinating the notification of an eligible data breach to the Privacy Commissioner and affected individuals; and
c. ensuring compliance with the record keeping obligations.

(51) Managers/Supervisors are responsible for:

a. ensuring individuals under their supervision undergo the Cyber Security training provided by the University, are aware of this Policy, the Privacy Policy, the Cyber Security Policy and related procedures; and
b. promptly reporting any data breaches, suspected data breaches, or policy violations by or reported to them, to the IT Service Desk, Cyber Security Team or Privacy Officer.

(52) Executive Group members are responsible for:

a. ensuring that, within their portfolio, there is training provided for Staff and manager/supervisors in data breach identification and management; and
b. if an eligible data breach is considered a critical incident, adopting their roles as members of the Critical Incident Management Team.

(53) The Vice-Chancellor is responsible for:

a. appointing one or more persons, as Assessors, to carry out the assessment as outlined in this Policy and determine whether a data breach is an eligible data breach based on the outcome of the assessment; and
b. approving an extension period for the assessment if satisfied it cannot reasonably be conducted within 30 days.

Section 4 - Guidelines

(54) Nil.

Section 5 - Definitions

(55) The following definitions apply for the purposes of this Policy:

a. Affiliate includes contractors, agents, visitors, honorary, clinical or adjunct appointees and consultants of the University.
b. Controlled Entity/Entities means a person, group of persons or body of which the University or the University Council has control within the meaning of Section 39 (IA) or 45A (IA) of the Government Sector Audit Act 1983 (NSW).
c. Health Information is as defined in the Health Records and Information Privacy Act 2002.
d. IT Service Desk means the Macquarie University IT function that provides direct IT support for Staff, Students, and other authorised users.
e. Personal Information is as defined in the Privacy and Personal Information Protection Act 1998 (NSW). For the purposes of the MNDB Scheme, Personal Information includes Health Information (that is, information about an individual's physical or mental health, disability and information connected to the provision of a health service.)
    i. Personal Information does not include(this list is not exhaustive):
        - information about an individual who has been dead for more than thirty (30) years;
        - information about an individual that is contained in a publicly available publication;
        - information or an opinion about an individual's suitability for appointment or employment as a public sector official; or
        - information about an individual that is contained in a public interest disclosure.
f. Privacy Commissioner refers to an independent regulator that deals with privacy issues that arise under the PPIP Act and the HRIP Act in NSW. Relevant Privacy Commissioners include:
    i. the Information and Privacy Commission NSW, when an eligible data breach has occurred impacting the University; or
    ii. the Office of the Australian Information Commissioner when an eligible data breach has occurred impacting the University's Controlled Entities under the NDB Scheme or where a University data breach relates to tax file numbers or Student fee data.
g. MNDB Scheme means the Mandatory Notification of Data Breach Scheme under Part 6A of the Privacy and

Personal Information Protection Act 1998 (NSW).

h. Staff means all persons employed by Macquarie University, including continuing, fixed term, and casual Staff members.

i. Student means any undergraduate, postgraduate, graduate research, or non-award Student currently enrolled or formerly enrolled at the University, whether based on or off-campus.

Status and Details

Status	Current
Effective Date	13th June 2024
Review Date	12th June 2027
Approval Authority	Vice-President, Professional Services
Approval Date	12th June 2024
Expiry Date	Not Applicable
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.