Data Breach Policy

Section 1 - Purpose and Scope

(1) The University of Queensland (UQ) is committed to the effective management of data and information that it collects and holds. UQ aims to ensure that data breaches do not occur, however when they do, UQ is committed to meeting its legal obligations.

(2) UQ is committed to robust management and control of information it collects, and to ensuring the security of information that it collects and holds. This Policy outlines UQ's activities to prevent data breaches, but also its response to data breaches which do occur.

(3) In recognition of those commitments, UQ will:

a. implement policies (including this Policy) and procedures detailing how the University manages data breaches
b. publish these policies and procedures on the University's website (refer to the Policy and Procedure Library)
c. have appropriate practices, procedures and systems in place to manage data breaches in compliance with its legal obligations.

(4) This Policy:

a. applies to all UQ staff
b. does not apply to the controlled entities of the University. Boards of those entities must implement their own policies, consistent with their legal obligations.

Section 2 - Principles and Key Requirements

Prevention and preparation

(5) UQ will implement preparatory actions to enable early identification of and appropriate response to data breaches. This will be achieved through:

a. ensuring appropriate policies, procedures and systems are in place to:
    i. identify data breaches and report them appropriately
    ii. respond to data breaches, including appropriate mitigation and containment, assessments, notification and review
b. identifying specific reporting lines, internal decision makers and escalation points attached to controls and other mechanisms used to identify data breaches and respond to data breaches
c. ensuring there is a broad awareness across UQ of the policies, procedures and obligations.

(6) UQ is committed to maintaining a current awareness and knowledge of data breach management and privacy principles, and will deliver education and training activities to support that commitment.

This document may be varied, withdrawn or replaced at any time.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 refer to The University of Queensland's Policy and Procedure Library for the latest version.

Reporting and early containment of data breaches

(7) Any actual or suspected data breaches must be reported immediately to a Privacy Officer, through the University's Privacy website or by email to privacy@uq.edu.au.

(8) UQ Staff who identify an actual or suspected data breach should refer to the Data Breach Procedure for details on:

a. the information that should be reported to a Privacy Officer
b. how they should contain and mitigate the data breach
c. their other responsibilities in respect of management of the data breach.

UQ's response to data breaches

(9) UQ has established a Data Breach Committee responsible for oversight of:

a. governance relating to data breaches occurring at the University, including this Policy and its supporting procedures and processes
b. operational management of data breaches, with regular reporting from the Data Breach Response Team and Privacy Officer
c. appropriate planning, preparation and resourcing to manage data breaches.

(10) A Data Breach Response Team may be established by the Data Breach Committee in relation to data breaches to:

a. coordinate the operational management of data breaches including measures to contain and mitigate data breaches
b. provide reports to the Data Breach Committee in accordance with the Data Breach Procedure.

(11) UQ's management of data breaches involves distinct phases including:

a. identification and reporting – data breaches can be identified in a number of different ways, including:
    i. the identification of suspicious activity or a cyber security event
    ii. internal or external reporting, received by UQ through a telephone call, email or webform
    iii. the receipt of a complaint, through UQ's centralised complaints system or in some other way.

    This Policy and the Data Breach Procedure will embed UQ's reporting and governance oversight practices by ensuring data breaches are reported to a Privacy Officer and responded to appropriately.
b. containment and mitigation – the type of containment and mitigation activity required will depend on the type of breach that has occurred. Guidance on initial containment activities is provided in the Data Breach Procedure.

    Appropriate mitigation of data breaches will occur, having regard to the nature and severity of the breach, and consistent with UQ's Critical Incident Management Plan (available through the Enterprise Risk website), Cyber Security Incident Response Procedure and Data Breach Procedure.
c. assessment - assessments will be undertaken to determine whether there has been a data breach, having regard to the requirements of UQ's Data Breach Procedure. The assessment will consider multiple factors, including:
    i. whether the incident constitutes a critical incident to be managed in accordance with UQ's Critical Incident Management Plan
    ii. whether the incident is a cyber related event (and does not involve personal information) to be managed in accordance with the Cyber Security Incident Response Procedure

iii. whether the incident is a data breach and if so, whether it is an eligible data breach for the purposes of the Information Privacy Act 2009 having regard to the potential for serious harm to an individual).

If there is a reasonable suspicion that a data breach is an eligible data breach, an assessment must be completed within 30 days of forming the suspicion. However, if UQ cannot complete the assessment within this timeframe, acting reasonably, it may extend the assessment period.

Where UQ becomes aware that a data breach may affect another agency (as defined in the IP Act), it will give written notice to the other agency and discuss with the other agency who will lead the assessment requirements in compliance with the IP Act.

d. notification and reporting – if notification or reporting of a data breach is required by law, UQ will notify and report all data breaches in accordance with the legal requirements. This may include:
   i. reporting and notifications in relation to eligible data breaches pursuant to the IP Act
   ii. reporting cyber security incidents to the Australian Cyber Security Centre pursuant to the Security of Critical Infrastructure Act 2018.
e. monitoring and review – Each data breach will be included in reporting to the Data Breach Committee, with more detailed analysis regarding eligible data breaches (considering an incident report, including lessons learned), to establish what steps, if any, can be taken to prevent similar breaches occurring.

Section 3 - Roles and Responsibilities

Vice-Chancellor

(12) The Vice-Chancellor is ultimately accountable for ensuring the University meets its privacy obligations and does this through oversight of the application of policies and procedures designed to satisfy those obligations through regular reporting mechanisms.

UQ Staff

(13) UQ staff are responsible for:

a. promptly reporting any actual or suspected data breaches, as set out in this Policy
b. responding to any enquiries from a Privacy Officer or the Data Breach Response Team in respect to any suspected or actual data breach
c. fully participating in the assessment of a data breach
d. undertaking any appropriate containment activities, in accordance with the Data Breach Procedure and any guidance provided by a Privacy Officer or the Data Breach Response Team.

Data Breach Committee

(14) The Data Breach Committee (comprising the Chief Operating Officer (as Chair), Chief Information Officer, Director, Governance and Risk and Director, Integrity Unit, together with other relevant senior executives as required) is responsible for:

a. oversight of the governance relating to data breaches at the University
b. determining whether a data breach is an eligible data breach, based on advice from the Privacy Officer or Data Breach Response Team
c. oversight of the management of any data breaches which occur at UQ
d. determining the seriousness of any breach and appropriate actions to respond to it, including referral to the

Complaints Management Committee requesting an investigation by the Integrity Unit

e. considering reports on data breaches occurring at the University, their causes and consequences, how they are being managed
f. identifying any lessons learned from data breaches and implementing additional controls to prevent similar occurrences in the future.

(15) The Data Breach Committee will receive support from the Director of Cybersecurity, Director of Infrastructure Operations, Associate Director, Enterprise Risk and Compliance, Associate Director, Governance and Policy and other UQ staff as required.

Chief Operating Officer

(16) The Chief Operating Officer is accountable for:

a. overseeing and ensuring UQ's compliance with its privacy obligations as they relate to data breaches
b. developing, implementing and maintaining this Policy and any accompanying procedures to ensure that UQ can demonstrate compliance with its obligations as they relate to data breaches
c. ensuring appropriate notifications are made pursuant to UQ's legal obligations in relation to data breaches
d. reporting to the Senate Risk and Audit Committee and University Senior Executive Team with respect to the University's compliance with this Policy
e. ensuring UQ staff have access to appropriate training materials and resources in relation to data breaches and breach responses.

Data Breach Response Team

(17) The Data Breach Response Team will be a multi-disciplinary team, having regard to the specific nature of the data breach. The team will usually comprise a Privacy Officer, the Information Custodian, and other relevant stakeholders from across the University (including Legal Services, Marketing and Communication, Enterprise Risk Services and Information Technology Services as required).

(18) The Data Breach Response Team will be responsible for:

a. coordination of activities to contain or mitigate an actual or suspected data breach
b. operational management of the response strategy for an actual or suspected data breach, in accordance with the Data Breach Procedure
c. reporting to the Data Breach Committee.

Privacy Officer

(19) A Privacy Officer is responsible for:

a. undertaking threshold assessments in accordance with clause 11(c) of this Policy to determine the nature of the data breach and how best it should be managed, including:
    i. working with the Cyber Security Operations Centre in the case of cyber security incidents
    ii. making recommendations to the Data Breach Committee as to whether a Data Breach Response Team should be established
b. in circumstances where suspected breaches have been identified;
    i. coordinating the Data Breach Response Team as required
    ii. reporting to the Data Breach Committee
c. maintaining a register of actual and suspected data breaches, including any registers required under the IP Act

d. providing advice and support, to UQ Staff and the broader community, in relation to UQ's management of data breaches
e. participating in UQ's processing of and response to data breaches, in accordance with this Policy.

Section 4 - Monitoring, Review and Assurance

(20) Monitoring of the effectiveness of this Policy will be undertaken by way of:

a. collation and analysis of relevant data. For example, this might include statistics relating to how many times the Policy has been accessed, training provided in relation to the Policy, notifications made by staff having regard to the requirements of the Policy, complaints and the occurrence of suspected or actual data breaches
b. feedback from users of the Policy (either internal or external).

(21) UQ has established a range of measures to enable it to prepare for and respond to data breaches including:

a. mandatory staff training on UQ's privacy obligations
b. internal resources to help staff to identify and report any suspected or actual data breaches.

(22) The Chief Operating Officer is responsible for ensuring that this Policy is regularly reviewed, having regard to the requirements of the regulatory framework relative to data breaches, and the monitoring undertaken pursuant to clause 20.

(23) Assurance activities will be undertaken:

a. through the incident report completed after each data breach
b. through quarterly reporting by the Chief Operating Officer to the University Senior Executive Team and the Senate Risk and Audit Committee as outlined in this policy
c. through monitoring compliance with Policy by the policy owner
d. as required, by UQ's Internal Audit function to consider the effectiveness of this Policy and controls established to support it.

Section 5 - Appendix

Definitions

Defined Term	Meaning
Data breach	As defined in the IP Act is where, in relation to information held by UQ, there has been either: - unauthorised access to, or unauthorised disclosure of, the information; or - the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
Eligible data breach	As defined in the IP Act is a data breach where personal information held by UQ is: - accessed or disclosed without authorisation and this is likely to result in serious harm to the individual that it relates to; or - lost, and unauthorised access or disclosure is likely, and this is likely to result in serious harm to the individual that it relates to.
IP Act	The Information Privacy Act 2009 (Qld).

Defined Term	Meaning
Personal information	As defined in the IP Act to be information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: - whether the information or opinion is true or not; and - whether the information or opinion is recorded in a material form or not.
Privacy Officer	The UQ staff who have day to day responsibility for the management of privacy matters, including privacy complaints.
QPPs	The Queensland Privacy Principles as set out in Schedule 3 of the IP Act.
Serious harm	As defined in the IP Act: - Serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure; or - Serious harm to the individual's reputation because of the access or disclosure.
Unauthorised access	Information held by UQ is accessed by someone who is not authorised to do so.
Unauthorised disclosure	Intentional or unintentional disclosure, without permission, of personal information held by UQ
UQ Staff	Includes: - members of the UQ Senate - all UQ employees, including continuing, fixed-term, research (contingent funded) and casual employees - persons acting in an honorary or voluntary capacity for or at UQ, including work experience students - affiliates.

Status and Details

Status	Current
Effective Date	1st July 2025
Review Date	1st July 2028
Approval Authority	Vice-Chancellor and President
Approval Date	22nd June 2025
Expiry Date	Not Applicable
Policy Owner	Andrew Flannery Chief Operating Officer
Enquiries Contact	Office of the Chief Operating 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 refer to The University of Queensland's Policy and Procedure Library for the latest version.