Data Breach Procedure

Section 1 - Purpose and Scope

(1) This Procedure supports the Data Breach Policy and outlines the processes for the identification, reporting and initial mitigation of data breaches which occur in relation to information held by UQ.

(2) This Procedure applies to all UQ Staff.

(3) This Procedure is consistent with and complements other response plans and procedures, including the Critical Incident Management Plan (staff login required, via the Enterprise Risk website) and the Cyber Security Incident Response Procedure.

Section 2 - Process and Key Controls

(4) Data breach management at UQ is managed by various stakeholders depending on the nature of the data breach and relies on collaboration between organisational units and functions across UQ.

(5) UQ Staff are responsible for reporting any data breaches in accordance with the Data Breach Policy and this Procedure.

(6) The decision on how to respond to a data breach should be made on a case-by-case basis by applying the Data Breach Policy, this Procedure and any other relevant response plan or procedure.

(7) Where a data breach occurs, other UQ policies, plans and procedures might also be triggered.

> For example:
>
> a. where the data breach is also a critical incident: the Critical Incident Management Plan. The plan will guide the Critical Incident Management Team in anticipating, responding to, recovering and learning from critical incidents that may negatively impact UQ.
>
> b. where the data breach relates to a cyber event: the Cyber Security Incident Response Procedure. The Procedure will guide UQ's response to the cyber security incident.
>
> c. where the data breach relates to corrupt conduct: the Fraud and Corrupt Conduct Policy and Fraud and Corrupt Conduct Procedure. The Policy and Procedure will set out how UQ will assess and deal with complaints or information about the corrupt conduct.

(8) This Procedure should be read in conjunction with other policies, plans and procedures and may complement those processes.

> For instance, if the data breach is also a cyber breach, then the Cyber Security Incident Response Procedure will be activated, but this Procedure will also require that (not exhaustive):

a. where the data breach relates to personal information, then the nature of the breach must be assessed to establish if it is an eligible data breach in accordance with the Data Breach Policy and this Procedure.

b. a Data Breach Response Team may be established to ensure the data breach is sufficiently managed having regard to UQ's legal obligations.

c. reporting to the Data Breach Committee occur.

Section 3 - Principles and key requirements

Part A - Identification and reporting of an actual or suspected data breach

(9) A data breach can occur in a number of ways, for example, where:

a. there has been the physical loss of a device or documents
b. suspicious activity or a cyber security incident is identified
c. mistaken communications have occurred (e.g. email sent to the wrong email recipient)
d. there has been a system error.

(10) A data breach extends to any information held by UQ, including (but not limited to):

a. an individual's personal information
b. commercially sensitive information (i.e. data that is not intended for public disclosure such as business strategies, financial records or proprietary information)
c. personal information UQ controls even though it is in the possession of a third party (e.g., under a contract with a software as a service supplier that holds UQ data).

(11) All UQ Staff should consider whether an actual or suspected data breach may have occurred when it appears that there may have been:

a. unauthorised access to, or unauthorised disclosure of, information; or
b. loss of information in circumstances where unauthorised access to, or unauthorised disclosure is likely to occur.

(12) If an actual or suspected data breach is identified, staff must:

a. if also a potential cyber security incident, report the actual or suspected data breach through the Tell us about a cyber security concern or incident website
b. report the actual or suspected data breach to a Privacy Officer, either through UQ's Privacy website or by email to privacy@uq.edu.au
c. provide as much information as possible to enable an early assessment of the data breach. If known, the information provided should include:
    i. the time and date, duration and location of the actual or suspected breach
    ii. the type of information that may have been accessed, disclosed or lost
    iii. how the actual or suspected breach was discovered and by whom
    iv. how the actual or suspected breach occurred
    v. the extent of the breach
    vi. who is affected by the breach and the likely number of affected individuals

vii. any other relevant information

d. inform their direct supervisor of the identification of an actual or suspected data breach
e. be careful not to destroy evidence that may be valuable in determining the cause of the data breach or that would allow UQ to take appropriate corrective action
f. preserve records of the actual or suspected data breach
g. not compromise the ability of law enforcement agencies to investigate the breach (for example, by making details of the breach public too early)
h. take action to contain and mitigate the data breach in accordance with Part B (Containment and mitigation).

(13) If staff are unsure as to whether an actual or suspected data breach has occurred, or they need guidance on the immediate type of containment action to take, contact a Privacy Officer through the UQ Privacy website or at privacy@uq.edu.au.

Part B - Containment and mitigation

(14) When an actual or suspected data breach is identified, UQ Staff must consider whether any appropriate actions can be undertaken to contain the data breach. In doing so, care should be taken to ensure that any containment activity does not destroy information that might be needed to investigate the breach and prevent a recurrence.

(15) Some examples of potential containment options are outlined below:

Data breach	Possible containment option
Email containing personal information sent to incorrect recipient.	Ask the recipient to delete the email and request that the recipient confirms deletion of the information in writing.
Internal system releasing personal information incorrectly.	Contact ITS immediately to suspend the system and stop all data release. This can be done by contacting the application technical owner (or submit an ITS Support Request).
Unauthorised access to a work computer. **	Report a cyber security concern immediately to ITS, and ask them to change passwords and any other access requirements to the computer.
Unauthorised access to a work database containing personal information. **	Report a cyber security concern immediately to ITS, and ask them to review all users with access to the database and restrict access as necessary. ITS may also need to consider changing passwords to access the database.
Cyberattack/phishing attack/ malicious actor **	Report a cyber security concern immediately to ITS.
Lost device	Report a cyber security concern immediately to ITS.

** Reports to ITS and Cyber Security can be made through the Tell us about a cyber security concern or incident website.

(16) UQ Staff are encouraged to:

a. seek advice and support from a Privacy Officer, their supervisors and UQ Cyber Security Operations Centre in the case of cyber incidents in relation to appropriate containment of data breaches
b. treat all information about the incident as confidential and disseminate it on a strictly need-to-know basis only.

Part C - Assessment of the data breach

(17) Upon notification of a data breach, a Privacy Officer will conduct an initial assessment to determine the most appropriate way to manage the breach, having regard to the nature of the breach. This assessment will include:

a. whether the breach is sufficiently severe to require management by UQ Critical Incident Management Team. This assessment will be undertaken in consultation with Governance and Risk Division
b. whether to notify UQ's Cyber Security Operations Centre
c. whether the breach involves the unauthorised access to or disclosure or loss of personal information and should be managed in accordance with:
    i. the Cyber Security Incident Response Procedure
    ii. this Procedure
    iii. the Complaints Management Policy.

(18) When there is a data breach that does involve the unauthorised access to or disclosure or loss of personal information, the Privacy Officer may identify and recommend to the Data Breach Committee that a Data Breach Response Team be established to manage the response to incidents.

This approach is recommended particularly for incidents where a multi-disciplinary response is required.

By way of example, a Data Breach Response Team could include representation from Information Technology Services, Governance and Risk Division, Legal Services, Marketing and Communications, the Information Domain Custodian and a Privacy Officer to ensure a considered and managed response.

(19) Where a Data Breach Response Team is established, it will:

a. develop a coordinated plan to manage the data breach. This may include further containment or mitigation steps.
b. liaise with any relevant stakeholders to collect as much information as possible and identify:
    i. the time and date, duration and location of the actual or suspected breach
    ii. the type of information that may have been accessed, disclosed or lost
    iii. how the actual or suspected breach was discovered and by whom
    iv. how the actual or suspected breach occurred
    v. the extent of the breach
    vi. who is affected by the breach and the likely number of affected individuals
    vii. other relevant information.
c. as more information becomes available, consider whether to activate other response plans and procedures, such as:
    i. Critical Incident Management Plan
    ii. Cyber Security Incident Response Procedure
    iii. Fraud and Corrupt Conduct Policy and Fraud and Corrupt Conduct Procedure
    iv. Privacy Policy
    v. Staff Code of Conduct Policy.
d. determine whether any other stakeholders should to be engaged.
e. assess if personal information may be involved and where a data breach contains personal information:
    i. assess if the data breach is an eligible data breach for the purposes of the IP Act
    ii. in the instance where it is not clear whether a data breach is an eligible data breach, within 30 days of forming a suspicion that it is, assess whether there are reasonable grounds to believe that a data breach is an eligible data breach for the purposes of the IP Act.
f. with respect to time periods under the IP Act regarding data breach:
    i. monitor time periods and extensions

ii. advise the Data Breach Committee and policy owner of the Data Breach Policy of time periods and extension options and obligations
iii. provide assistance in relation to notifying regulators of extensions to time periods and providing other information required.

g. prepare reports for the benefit of the Data Breach Committee and ultimate decision-making by a delegate (where required).

(20) Where the data breach relates to personal information and the Data Breach Response Team has not been established, the Privacy Officer will:

a. assess if the data breach is an eligible data breach for the purposes of the IP Act
b. in the instance where it is not clear whether a data breach is an eligible data breach, within 30 days of forming a suspicion that it is, assess whether there are reasonable grounds to believe that a data breach is an eligible data breach for the purposes of the IP Act
c. attend to the other matters in clause 19
d. prepare reports for the benefit of the Data Breach Committee and ultimate decision-making by a delegate (where required).

(21) The Data Breach Committee is responsible for:

a. deciding whether a Data Breach Response Team should be established in respect of a particular data breach
b. determining, based on assessment reports prepared by the Data Breach Response Team or Privacy Officer relating to a suspected or actual eligible data breach, whether they are satisfied that the breach is an eligible data breach for the purposes of the IP Act
c. providing assurance regarding the integrity of the Eligible Data Breach Register (see clause 23).

Part D - Notification and reporting

(22) Where required by law, data breaches will be reported in accordance with legal requirements. Relevant requirements may include (but are not limited to):

a. Information Privacy Act 2009 (Qld), which requires that particular individuals and the Office of the Information Commissioner is notified where a data breach is known or reasonably believed to be an eligible data breach
b. Crime and Corruption Act 2001, which requires that the Crime and Corruption Commission is notified of matters where conduct is reasonably suspected to amount to corrupt conduct
c. Privacy Act 1988 (Cth), which requires that particular individuals and the Australian Information Commissioner is notified where there is an eligible data breach (for the purposes of that legislation as it applies to UQ)
d. Security of Critical Infrastructure Act 2018, which requires that UQ notifies the Australian Cyber Security Centre about significant incidents.

(23) The Privacy Officer is responsible for maintaining the Eligible Data Breach Register as required by the IP Act.

Part E - Monitoring and review

(24) After each actual or suspected data breach, the Privacy Officer, in consultation with key stakeholders and the Data Breach Response Team (where applicable) will prepare a report for the Data Breach Committee outlining:

a. the details of the data breach, including the information that may have been accessed, disclosed or lost and the extent of the breach including who was affected by the breach

b. the lessons learnt from the data breach
c. any improvements or controls that may have been put in place to prevent the breach from re-occurring or mitigating its impact
d. where improvements or controls are yet to be put in place, an action plan of who is responsible for implementing them
e. any legal or commercial issues for UQ (for instance any liability, compensation, insurance and other regulatory issues coming to light as a result of the data breach, excluding privileged legal advice and confidential matters.

(25) Quarterly reports will be prepared and presented to the University Senior Executive Team and the Senate Risk and Audit Committee outlining the data breaches that have occurred over the previous quarter, the actions taken to contain and mitigate those breaches, with additional information about data breaches that meet the threshold of being eligible data breaches under the IP Act.

Section 4 - Roles, Responsibilities and Accountabilities

Vice-Chancellor

(26) 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

(27) UQ Staff are responsible for:

a. promptly reporting any actual or suspected data breaches, as set out in this Procedure
b. responding to any enquiries from a Privacy Officer or the Data Breach Response Team in respect of 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 this Procedure and any guidance provided by a Privacy Officer or the Data Breach Response Team.

Data Breach Committee

(28) The Data Breach Committee comprises:

a. Chief Operating Officer (as Chair)
b. Chief Information Officer
c. Director, Governance and Risk
d. Director, Integrity Unit
e. other relevant senior executives as required.

(29) The Data Breach Committee 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 to request an investigation by the Integrity Unit
e. considering reports on data breaches occurring at the University, their causes and consequences, and how they are being managed
f. identifying any lessons learned from data breaches and implementing additional controls to prevent similar occurrences in the future.

(30) The Data Breach Committee will receive support from the Director of Cyber Security; Director of Infrastructure Operations; Associate Director, Risk; Associate Director, Governance and Policy; and other UQ Staff as required.

Chief Operating Officer

(31) 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 Procedure 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 University Senior Executive Team and Senate Risk and Audit Committee with respect to the University's compliance with this Procedure
e. ensuring UQ Staff have access to appropriate training materials and resources in relation to data breaches and breach responses.

Data Breach Response Team

(32) 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 Domain Custodian, and other relevant stakeholders from across the University (such as Legal Services, Marketing and Communications, Governance and Risk, and Information Technology Services).

(33) 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 this Procedure
c. reporting to the Data Breach Committee.

Privacy Officer

(34) A Privacy Officer is responsible for:

a. undertaking initial assessments in accordance with clause (17) of this Procedure 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 data breaches have been identified;
    i. coordinating and working with the Data Breach Response Team as required
    ii. reporting to the Data Breach Committee unless a Data Breach Response Team has been established
c. maintaining a register of actual and suspected data breaches, including the Eligible Data Breach Register and

any other 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 Procedure.

Section 5 - Monitoring, Review and Assurance

(35) The Chief Operating Officer will:

a. periodically review this Procedure to ensure its ongoing relevance
b. annually assess the effectiveness of this Procedure and provide assurance to the University Senior Executive Team.

Section 6 - 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).
Personal information	As defined in the IP Act, to be information about, 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.
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	Including: - 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	25th July 2025
Review Date	25th July 2028
Approval Authority	Chief Operating Officer
Approval Date	24th July 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.