Data Breach - Procedures

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

3 December 2024

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2026

STATUS

Active

1. Purpose

1.1 These procedures outline the process for a structured and coordinated response that mitigates impact, should a data breach transpire.

1.2 These procedures outline the University's response which considers 9 essential elements in protecting against and managing data breaches, being to minimise impact, comply with legislation, ensure an efficient and coordinated response, notify and communicate with the relevant persons and authorities, contain and remediate, recover data, mitigate risk and prevent for the future, train and ensure procedural awareness and strive for continuous improvement.

1.3 These procedures are supplemented by the University's Data Breach Response Plan (login required) and address the legislative requirements of the *Information Privacy Act 2009 (Qld)* and the *Privacy Act 1988 (Cth)*.

1.4 These procedures must be read in conjunction with the linked Data Governance – Operational Policy, Data Management - Procedures, Data Handling – Guidelines (login required).

2. Scope and application

2.1 These procedures apply to all University staff, students undertaking research or involved in other University business, approved third parties, alumni, contractors, and sub-contractors. It includes all individuals who handle University data and information, regardless of their role or affiliation.

2.2 These procedures apply to all University data and information.

2.3 Suspect, potential and verified data breaches are in scope of these procedures.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

3.2 The terms data and information are used interchangeably within this policy, recognising the overlap between the two. In their simplest form, data is often considered as raw values and individual facts in any form, and information is data that has been contextualised. Both data and information can be University records.

4. Response phases in managing data breaches

4.1 There are four phases to responding to data breaches:

(a) Phase 1: Preliminary identification and detection;

(b) Phase 2: Initial investigation and assessment;

(c) Phase 3: Remediation and action plan; and

(d) Phase 4: Review and recovery.

4.2 Phase 1: Preliminary identification and detection

4.2.1 University staff who have identified a data breach must undertake the key steps as identified in Figure 1: Preliminary identification and detection steps.

Figure 1: Preliminary identification and detection steps

4.2.2 University staff who identify a data breach must take immediate steps for containment to minimise harm and impact. This can include recalling an email or contacting the IT Service Desk (login required) to report technical or University system vulnerability.

4.2.3 Evidence about the data breach must be captured via the Data Breach Report Form (login required)which captures information on type, classification of data and how it appears to have occurred.

4.2.4 When a student or third party detects a data breach, they must report it via a staff member using formal channels. Staff should prioritise timely reporting over form completeness.

4.2.5 Submitting the form activates the specialist Data Breach Triage Team (DBTT), who commences an investigation.

4.2.6 Advice and supporting documentation for containing, recording, and reporting suspected breaches are available on the University Data Portal (login required), ensuring staff are equipped to act effectively.

4.3 Phase 2: Initial investigation and assessment

4.3.1 The initial examination process, which is led by the DBTT, requires undertaking the key steps as identified in Figure 2: Initial investigation and assessment steps.

Figure 2: Initial investigation and assessment steps

4.3.2 Dependent on the initial assessment by the DBTT, a data breach is either managed by the DBTT, or escalated to the Data Breach Incident Response Team (D-BIRT) or the University's Incident Response Team (IRT).

4.3.3 Escalation is based on risk, with a process to identify in the Data Breach Response Plan (login required). The decision to escalate a data breach is informed by factors including:

(a) the assessment of harm;

(b) compliance requirements;

(c) the nature of the breach;

(d) the involvement of personal information; and

(e) the number of impacted individuals.

4.3.4 The Chief Data Officer (CDO) is responsible for the decision to escalate a data breach and is informed by the initial assessment findings.

4.4 Phase 3: Remediation and action plan

4.4.1 The responsible response team identified in Phase 2 must develop and implement a structured remediation and action plan tailored to the unique circumstances of the data breach, in accordance with the Data Breach Response Plan (login required).

4.4.2 This ensures all required actions are identified, clearly documented, and assigned to the relevant teams or individuals to be completed.

4.4.3 When multiple teams are involved (e.g. to coordinate a data breach that is the result of a cyber security incident), teams must communicate on the status and ownership of actions to ensure the process is streamlined. Guidance for coordination when multiple teams are involved in the response is provided in the Data Breach Response Plan (login required).

4.4.4 Ongoing or operational risks identified during the response must be communicated and assigned to the relevant business area for management and risk treatment, in accordance with the Risk Management - Governing Policy. These risks should be recorded in the appropriate register for continuous monitoring.

4.4.5 Data breach notification requirements

4.4.5.1 Data breach notification requirements are dependent on the nature of the data breach. The CDO is responsible for ensuring all data breach notifications are managed in accordance with the Data Breach Response Plan (login required).

4.4.5.2 The University can be required to notify affected individuals, regulatory authorities, or make public notifications, based on the:

(a) type of data breached;

(b) risk of harm;

(c) number of individuals impacted; or

(d) method by which the data was breached.

4.4.5.3 The University is committed to acting transparently and in compliance with the *Information Privacy Act 2009 (Qld), Privacy Act 1988 (Cth)*, and other relevant legislation when managing data breach notifications.

4.4.5.4 Notification obligations for international jurisdictions must be considered on a case-by-case basis, as required.

4.5 Phase 4: Review and recovery

4.5.1 Once the data breach has been resolved, a review must be undertaken to capture lessons learned and assess the effectiveness of the process to improve future responses.

5. Response teams

5.1 Coordination of the response to a data breach is handled by specialised teams that are mobilised based on the nature of the reported data breach and stage in the response. An overview of these teams is provided in Table 1: University response teams and their requirements.

Table 1: University response teams and their requirements

RESPONSE TEAM	RESPONSE TEAM REQUIREMENTS
Data Breach Triage Team (DBTT)	(a) Undertakes initial triage of all data breaches; (b) Coordinates response to non-critical incidents that carry low risk; (c) Escalates to D-BIRT when required.
Data Breach Incident Response Team (D-BIRT)	(a) Coordinates response to non-critical incidents that carry medium to high risk; (b) Escalates to the University's IRT when required; (c) Supports the University's IRT in response to critical incidents.
University Incident Response Team (IRT)	(a) Coordinates response to critical incidents of high or extreme risk and moderate or higher consequence (as per the Critical Incident Management - Operational Policy).
Cyber Security Incident Response Team (CSIRT)	(a) Coordinates technical response related to cyber security events; (b) Works in parallel with D-BIRT or the University IRT on data breaches that involve a cyber security incident.

5.2 Full details of these teams, including membership and responsibilities, is provided in the Data Breach Response Plan (login required).

6. Intersection between data breach and cyber security incident

6.1 Cyber security incidents can result in a data breach, but a data breach does not have to be the result of a cyber security incident.

6.2 When a data breach is also a cyber incident, a coordinated response is essential, requiring collaboration between the D-BIRT and CSIRT, in accordance with the Data Breach Response Plan (login required).

6.3 When a data breach also involves a security breach of University business systems, staff reporting the data breach should also submit a report to the IT Support Desk (login required).

7. Monitoring and reporting

7.1 Regular monitoring and reporting on the application of the Data Breach – Procedures is reported to the Data Analytics and Information Management Advisory Committee.

7.2 The Chief Data Officer monitors and reports on University compliance with these procedures in accordance with the Compliance Management Framework - Governing Policy.

8. Authorities and responsibilities

8.1 As the Approval Authority the Chief Operating Officer approves these procedures to operationalise the Data Governance – Operational Policy.

8.2 As the Responsible Executive Member the Chief Operating Officer can approve guidelines to further support the operationalisation of these procedures. All procedures and guidelines must be compatible with the provisions of the policy they operationalise.

8.3 As the Designated Officer of these procedures the Chief Data Officer is authorised to approve associated documents to support the application of these procedures.

8.4 These procedures operate from the last amended date, with all previous iterations of data breach policy documents replaced and having no further operation from this date.

8.5 All records relating to data breach management must be stored and managed in accordance with Records Management – Procedures.

8.6 These procedures must be maintained in accordance with the Policy Framework - Procedures and reviewed on the shortened 2-year policy review cycle.

8.7 Any exception to these procedures to enable a more appropriate result must be approved in accordance with the Policy Framework - Procedures prior to any deviation from these procedures.

8.8 Refer to Schedule C of the Delegations Manual in relation to the approved delegations detailed within these procedures.

8.9 Data Breach Roles

8.9.1 The roles and their responsibilities outlined below in Table 2: Roles, responsibilities, and accountabilities, comprise a robust approach to effectively manage and mitigate data breaches.

Table 2: Roles, responsibilities, and accountabilities

ROLE	POSITION	RESPONSIBILITY AND ACCOUNTABILITY
Chief Data Officer	Chief Data Officer	Accountable for: (a) management of data breaches; (b) implementation of a Data Breach Response Plan for management of the response to data breaches; and (c) overseeing compliance with privacy and data protection legislation relevant to data breaches. Responsible for: (a) coordination and communication efforts during data breaches; (b) ensuring required notifications are made to regulators and impacted individuals, in accordance with the Data Breach Response Plan; (c) implementing data breach risk mitigation, rapid response and recovery strategies to uphold data security and compliance; (d) ensuring adherence to the Data Breach Response Plan during data breach responses; (e) appointing Data Custodians and ensuring their awareness of data breach responsibilities; and (f) driving strategic decisions and continuous improvement for data breach management.
Data Custodian	Heads of Departments (appointed by CDO)	Responsible for: (within their data domain) (a) raising awareness for timely reporting of data breaches; (b) leading immediate response and remediation actions for data breaches; and (c) monitoring and managing data security and integrity within data domain, identifying and addressing risks.
Business System Owner	In accordance with the ICT Security - Operational Policy	Responsible for:

		(a) ensuring business systems are secure to protect against data breaches; and (b) overseeing implementation of technical safeguards and recovery processes post-incident.
Data Subject Matter Expert	Staff based on specific expertise-criteria relative to a data asset	Responsible for: (a) providing expertise on assessing the impact of a data breach; and (b) recommending containment and corrective measures.
Data User	All University staff and/or groups and individuals that create or use data	Responsible for: (a) following protocols for breach detection and reporting; (b) adhering to these procedures; and (c) upholding the university's overall data security measures.

END

RELATED DOCUMENTS

• Acceptable Use of ICT Resources - Operational Policy

• Compliance Management Framework - Governing Policy
• Compliance Management Framework - Procedures
• Critical Incident Management - Operational Policy
• Data Classification - Procedures
• ICT Security - Operational Policy
• Incident Management - Procedures
• Privacy and Right to Information - Operational Policy
• Privacy Management - Procedures
• Records Management - Procedures
• Right to Information - Procedures
• Risk Management - Governing Policy
• University Policy Documents - Procedures

LINKED DOCUMENTS

• Data Governance - Operational Policy

• Data Management - Procedures

RELATED LEGISLATION / STANDARDS

• Right to Information Act 2009 (Qld)
• Public Records Act 2023 (Qld)
• Spam Act 2003 (Cth)
• Information Privacy Act 2009 (Qld)
• Invasion of Privacy Act 1971 (Qld)