Data Breach Policy

Document No.	2.20	**Version**	2.0
Effective Date	10 August 2026		
Policy Owner	Chief Financial Officer		
Policy Author	General Counsel		
Approval Authority	Chief Executive Officer		
Next Review Date	1 August 2028		
Published Externally	Yes		

Policy Snapshot

This Policy sets out how Titles Queensland will identify, manage and respond to a Data Breach within Titles Queensland, including a suspected Eligible Data Breach, and ensure compliance with the *Information Privacy Act 2009* (Qld).

1. Policy objective

Titles Queensland must comply with the mandatory notification of Data Breach (**MNDB**) scheme under the IP Act to the extent that it is performing titles registry functions. As required under the MNDB scheme, Titles Queensland has established systems and processes for effectively identifying, containing and mitigating, assessing, notifying and reviewing Data Breaches, including suspected Eligible Data Breaches. These systems and processes are set out or referred to in this Policy.

2. Key terms/ definitions

Affected Individual	has the same meanings as in section 47(1)(ii) of the IP Act.
Data Breach	means a security incident in relation to information held by Titles Queensland in the performance of a Titles Registry Function, involving either of the following: (a) unauthorised access to, or unauthorised disclosure of, the information; or

	(b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.
Data Breach Response Team	includes the General Counsel or delegate and Head of Risk and Compliance with inclusion of relevant subject matter experts as required based on the nature of the Data Breach.
Eligible Data Breach	occurs under section 47 of the IP Act where: (a) there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or (b) there has been loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information and the loss is likely to result in serious harm to any of the individuals to whom the information relates.
Eligible Data Breach Register	means the register of Eligible Data Breaches kept by Titles Queensland in accordance with section 72 of the IP Act.
Enabling Act	means the *Queensland Future Fund (Titles Registry) Act 2021* (Qld).
Employees	means all employees and contractors of Titles Queensland, whether on a full time, part time or casual basis.
Information Commissioner	means the Queensland Information Commissioner.
IP Act	means the *Information Privacy Act 2009* (Qld).
Personal Information	means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (a) whether the information or opinion is true or not, and (b) whether the information or opinion is recorded in a material form or not.
Policy	means this Data Breach Policy, as amended from time to time.
Serious Harm	to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's Personal Information, includes, for example: (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.
Titles Queensland	means Queensland Titles Registry Pty Ltd ACN 648 568 101.

Titles Registry Function	has the meaning given to it by section 5 of the Enabling Act.

3. Roles and Responsibilities

This Policy applies to all Employees. The following roles and/or groups have specific responsibilities for implementing this Policy:

Chief Executive Officer (or delegate)	• Ensure Titles Queensland complies with relevant legislation and policies regarding data breaches. • Approve and oversee the implementation of post-breach remediation actions.
Data Breach Response Team	• Coordinate the containment and mitigation measures in response to Data Breaches. • Follow this Policy when responding to a Data Breach. • Engage relevant internal and external subject matter experts as required. • Review and respond to data breaches impacting Titles Queensland's external service providers.
Employees	• Read this Policy and understand what is expected of them. • Comply with the IP Act, including protecting Personal Information held by Titles Queensland from unauthorised access, disclosure or loss. • Where required in accordance with this Policy, immediately report any actual or suspected Data Breach Incident through TitlesGRC. • Respond to requests for information from and cooperate with the General Counsel and/or the Data Breach Response Team. • Comply with record keeping obligations.
General Counsel (or delegate)	• Assess the severity of a Data Breach involving Personal Information and whether an Eligible Data Breach has occurred. • Escalate serious Data Breaches and all Eligible Data Breaches to the Chief Executive Officer and the Board. • Notify (or arrange to notify) the Information Commissioner, Affected Individuals and others where required.
Head of ICT	• Coordinate the technical containment and mitigation measures for Data Breaches.
Head of Risk and Compliance	• Maintain the Register of Eligible Data Breaches.

4. Data Breach Policy

Titles Queensland has established systems to respond to a Data Breach based on the following principles:

4.1 Stage 1 - Preparation

(a) Training and awareness

All Employees receive privacy and information security training and refresher training relevant to their role at Titles Queensland.

All new Employees must undertake privacy, information security and where relevant other training before they are granted access to Titles Queensland systems containing Personal Information.

(b) Testing

Titles Queensland maintains a testing and management program for its network and infrastructure (both digital and physical) to protect against Data Breaches, as well as ensuring robust security measures are in place including encryption, access controls and regular audits, testing and patching.

(c) Alignment with other policies

In addition to this Policy, Titles Queensland has detailed information security response plans, playbooks and frameworks that are maintained, including:

- Privacy Policy;
- Crisis Management Plan (and associated playbooks and incident management processes); and
- Business Continuity Plan.

4.2 Stage 2 - Identification

A Data Breach can occur in relation to any information held by Titles Queensland, not just Personal Information and at Titles Queensland, can include:

- a malicious cyber-attack on Titles Queensland's systems;
- information mistakenly published online;
- lost or stolen devices;
- lost or stolen paperwork or hard copies of documents;
- information mistakenly emailed to the wrong person; and
- a system error.

A suspected Data Breach may be identified internally (e.g. by an Employee or IT system alert) or externally (e.g. by a report from a member of the public or a government agency).

All Employees must immediately report any Data Breach or suspected Data Breach by logging a Data Breach Incident Report through TitlesGRC and documenting details of the incident. Employees should notify their manager and seek their assistance reporting the incident if required. The incident is then notified to the Data Breach Response Team.

4.3 Stage 3 - Contain and Mitigate

Upon receiving notification of a Data Breach or suspected Data Breach, the Data Breach Response Team will coordinate the evaluation and immediate steps to stop and/or limit the Data Breach, or implement measures to mitigate harm including, where appropriate:

- revoke or change access codes or passwords;
- restore/change locks if buildings may have been breached;
- secure, restrict access to, or shut down breached systems;
- suspend the activity that led to the Data Breach;
- run services on different IP addresses;
- ascertain whether the information has been shared or disseminated; and
- investigate whether copies of data have been made and, if so, take measures to ensure that all copies have been recovered, deleted or destroyed.

4.4 Stage 4 - Assess

Within 30 days of the identification of a Data Breach (or any longer period as approved by the Information Commissioner), the General Counsel or their delegate will assess whether there are reasonable grounds to believe that the incident is an Eligible Data Breach, having regard to the stated matters set out in the IP Act, including:

- the kind and sensitivity of Personal Information accessed, disclosed or lost;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the Personal Information;
- the nature of the harm likely to result from the Data Breach.

Based on the nature of the Data Breach, the assessment may need to be undertaken in conjunction with subject matter experts (internal or external).

4.5 Stage 5 - Notify

As soon as practicable after determining that a Data Breach is an Eligible Data Breach, and no relevant exemption applies, the General Counsel must notify:

- the Information Commissioner; and
- Affected Individuals.

Individuals will be notified and provided the required information (including recommendations about the steps individuals should take in response to the Eligible Data Breach) by one of the following methods:

- **Option 1 - Notify each individual**
  If it is reasonably practicable to notify each individual whose Personal Information was accessed, disclosed or lost by telephone, letter, email or in person.
- **Option 2 - Notify each Affected Individual**
  If Option 1 does not apply, notify each Affected Individual by telephone, letter, email or in person.
- **Option 3 - Publish Information**
  If neither Option 1 nor Option 2 apply, publish the required information on the Titles Queensland website for at least 12 months.

4.6 Stage 6 - Post Eligible Data Breach Review and remediation

For each identified Eligible Data Breach, the General Counsel will prepare an incident review report with relevant subject matter experts, and provide advice to the Chief Executive Officer or delegate, to coordinate the implementation of its recommendations to mitigate a recurrence of the Data Breach. The incident report will focus on mitigating risks of similar breaches by:

- analysing all aspects of the Eligible Data Breach to identify key learnings;

- specifying details of remediation activities determined by the nature and scale of the Eligible Data Breach; and
- recommending improvements to Personal Information handling processes.

5. Recordkeeping

The Head of Risk and Compliance will record details of all Eligible Data Breaches in the Eligible Data Breach Register with the information required by section 72 of the IP Act.

All data breach incidents, whether eligible or not, must be documented and retained in accordance with the *Public Records Act 2023* (Qld).

6. References

Information Privacy Act 2009 (Qld)
Public Records Act 2023 (Qld)
Queensland Future Fund (Titles Registry) Act 2021 (Qld)
2.17 Acceptable Use of IT Policy
2.18 Privacy Policy
3.08 Information Security Policy
Business Continuity Plan
Crisis Management Plan