Data Breach Policy

Document No.	2.20	**Version**	1.0
Effective Date	1 July 2025		
Policy Owner	Chief Operating & Legal Officer		
Policy Author	General Counsel		
Approval Authority	Chief Executive Officer		
Next Review Date	1 July 2026		
Published Externally	Yes		

Policy Snapshot

Titles Queensland collects, stores, uses and discloses information, including Personal Information, in performing the functions as operator of the land register, water allocations register and the foreign ownership of land register. This Policy sets out how Titles Queensland will respond to a Data Breach, including a suspected Eligible Data Breach as required under 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 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	means in relation to a: **Physical Data Breach:** Led by the Head of Risk and Compliance with inclusion of relevant subject matter experts as required. **Digital Data Breach:** Led by the Head of ICT with inclusion of relevant subject matter experts as required. Based on the nature of the Data Breach, additional internal and/or external subject matter experts will be engaged, including: • Chief Information Officer; • Chief Information Security Officer; • Chief Operating and Legal Officer; and • General Counsel.
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.
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.

3. Roles and Responsibilities

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

Chief Information Security Officer (CISO)	• Participate in managing a Data Breach with the Data Breach Response Team as a subject matter expert.
Chief People Officer (CPO)	• Ensure all Employees receive training and are aware of their responsibilities under this Policy.
Data Breach Response Team	• Coordinate the containment and mitigation measures in response to Data Breaches. • Engage relevant internal and external subject matter experts as required.
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 all Data Breaches or suspected Data Breaches to their immediate Manager and notify the ICT Support Team via the ICT portal and by telephone. • 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	• Participate in Data Breach Response Team as a subject matter expert.

	• 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	• Receive reported Data Breaches and Suspected Data Breaches. • Coordinate the containment and mitigation measures for digital Data Breaches. • Participate in Data Breach Response Team as a subject matter expert.
Head of Risk and Compliance	• Coordinate the containment and mitigation measures for physical Data Breaches. • Participate in Data Breach Response Team as a subject matter expert.
ICT Support Team	• Perform the initial triage and escalate reported Data Breaches or suspected Data Breaches to the relevant teams.

4. Data Breach Policy principles

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

4.1 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 and information security 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, including:

- penetration testing;
- threat intelligence monitoring;
- security patching; and
- regular exercises to test its Business Continuity Plan and other Incident Management processes.

(c) Alignment with other policies

In addition to this Policy, Titles Queensland has detailed information security response plans, playbooks and frameworks. Actions taken under this Policy may occur in conjunction with one or more of these, including Titles Queensland's:

- Privacy Policy;
- Crisis Management Plan;
- Data Breach Playbook;
- Technology Disruption Playbook;
- ICT Incident Management Process; and
- Business Continuity Plan.

4.2 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 to their immediate Manager and notify the ICT Support Team via the ICT portal and by telephone.

The ICT Support Team will escalate Data Breaches or suspected Data Breaches to the relevant members of the Data Breach Response Team to contain and mitigate.

4.3 Contain and Mitigate

Upon receiving notification of a Data Breach or suspected Data Breach, the Data Breach Response Team will coordinate the evaluation and steps to stop and/or limit the Data Breach, 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 Assess

Within 30 days of the identification of a Data Breach (or any longer period as approved by the Information Commissioner), the General Counsel 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, being:

- the kind of Personal Information accessed, disclosed or lost;

- the sensitivity of the Personal Information;
- whether the Personal Information is protected by one or more security measures and the likelihood that any of those security measures could be overcome;
- 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; and
- any other relevant matter.

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 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
- particular 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 Post Eligible Data Breach Review and remediation

For each identified Eligible Data Breach, the General Counsel will prepare an incident review report and provide advice to the Chief Executive Officer and relevant Executives and 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.

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

4.7 Register of Eligible Data Breaches

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