Queensland Competition Authority

Data Breach Policy

July 2025

Data Breach Policy

Version 1

Policy statement

The Queensland Competition Authority (QCA) is committed to the fair collection and safe handling of personal information in accordance with the *Information Privacy Act 2009* (Qld) (the IP Act).

The QCA's Data Breach Policy outlines our procedures for responding to a data breach, as required by section 73 of the IP Act.

1. Scope/application

This Data Breach Policy applies to all employees of the QCA. It should be read in conjunction with the Information Privacy Policy.

2. Definitions

Data breach

As defined in schedule 5 of the IP Act, a data breach means either of the following in relation to information held by the QCA:

(a) unauthorised access to, or unauthorised disclosure of, the information

(b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

Eligible data breach

Defined in section 47 of the IP Act (Box 1).

Box 1: Section 47 of the IP Act

(1) An *eligible data breach* of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if–

(a) both of the following apply–

(i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information;

(ii) the access or disclosure is likely to result in serious harm to an individual (an *affected individual*) to whom the personal information relates, having regard to the matters stated in subsection (2); or

(b) the data breach involves the personal information being lost in circumstances where–

(i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and

(ii) if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an *affected individual*) to whom the personal information relates, having regard to the matters stated in subsection (2).

(2) For subsection (1)(a)(ii) and (b)(ii), the matters are–

(a) the kind of personal information accessed, disclosed or lost; and

(b) the sensitivity of the personal information; and

(c) whether the personal information is protected by 1 or more security measures; and

(d) if the personal information is protected by 1 or more security measures– the likelihood that any of those security measures could be overcome; and

(e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and

(f) the nature of the harm likely to result from the data breach; and

(g) any other relevant matter.

3. Roles and responsibilities

Table 1 outlines the specific roles and responsibilities of teams and individuals in managing data breaches.

Table 1: Data breach responsibilities of QCA staff

Role	Responsibilities
QCA staff	Read the Data Breach Policy and Security Incident Response Plan and understand what is expected of them. Comply with the IP Act, including protecting personal information held by the agency from unauthorised access, disclosure or loss. Respond to requests for information from the Information Management Officer and/or the Incident Response and Crisis Management teams and cooperate with all of them. Comply with record keeping obligations.
Managers and Senior Leadership Team	Identify and escalate concerns within their area of responsibility that may trigger the requirements of the Data Breach Policy. Immediately report a data breach that is also a cyber security incident to the Incident Response Team, if not already reported.
Manager Information Technology	Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to any related individuals. Escalate serious data breaches to Incident Response and Crisis Management teams. Immediately report a data breach that is also a cyber security incident to the Incident Response Team, if not already reported. Report data breaches that are not serious to the senior leadership team and the Board via the regular reporting channels.
Information Management Officer	Maintain the Register of Eligible Data Breaches. Maintain and update the Data Breach Policy.
Incident Response Team	Investigate all reported actual and suspected data breaches. Assist the Manager Information Technology in assessing the severity of a data breach involving personal information. Escalate significant breaches to Crisis Management Team as necessary.
Crisis Management Team	Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems. Notify (or arrange for a senior officer or executive to notify) the Information Commissioner, affected persons and others where required. Conduct a post-breach review and do remediation. Read the IT Disaster Recovery Plan and Business Continuity Plan and understand what is expected of them.

4. Data breach management

4.1 Preparation

The QCA implements several procedures designed to protect privacy and secure the information held in physical and electronic formats under its control, and to help prevent unauthorised access and reduce any impact if unauthorised access does occur.

Physical security

- Premises are secured from unauthorised access.
- Staff access to areas where personal information may be stored is limited.
- A clean-desk policy is followed.

Technical solutions

- Access controls and audit logs are implemented.
- Activity-monitoring software is used.
- Threat and risk assessments are undertaken regularly.
- Staff are trained regularly in cybersecurity best practices.
- Third-party audits of systems are undertaken regularly.

Procedural

Review the following plans regularly according to a schedule:

- Security incident response plan
- IT disaster recovery plan
- Business continuity plan.

These internal plans help staff prepare for and respond to data breaches. They include information on roles and escalation procedures that are activated according to the severity of the breach.

4.2 Identification

As the causes and severity of data breaches can vary, detection and assessment activities are vital to both prevent a potential data breach, and to manage and mitigate an actual data breach. Importantly, data breaches do not happen exclusively because of the actions of third parties (malicious or otherwise) but can also result from human error – some examples are outlined in Table 2.

Table 2: Example causes of data breaches

Third-party actions	Human error
Theft of documents or storage devices from QCA premises	Accidental loss of documents or storage device
Phishing/malware/hacking attempts	Sending an email to unintended recipient/s

Third-party actions	Human error
Contractor disclosing sensitive personal information to external parties	Accidental access to confidential information

Software solutions have been implemented to help prevent, detect and assess data breaches involving information held in an electronic format. However, breaches of electronic systems can still happen.

Breaches can also occur with regards to physical documents, storage devices and similar items. Therefore, it is essential that all suspected or actual data breaches are reported immediately to the relevant contact listed in Table 3.

Table 3: Data breach reporting contacts

Reporting entity	Contact	Contact details
QCA staff	Incident Response Team	As in the Incident Response Plan
External stakeholder / the public	Manager Information Technology	Online QCA contact form*

* https://www.qca.org.au/contact/

Table 2 outlines the preferred contact methods to ensure all material facts are recorded in writing. If you believe that a data breach, or suspected data breach, is likely to cause both immediate and significant harm, please call the QCA directly on 07 3222 0555.

The signs and causes of data breaches will vary depending on how serious and widespread the breach is, so include as many details as possible when reporting the breach. Reports will be assessed to confirm that a data breach has occurred – and if so, whether the breach is to be considered an eligible data breach (s. 47).

4.3 Containment and mitigation

When a data breach is discovered, the QCA will take immediate and ongoing steps to limit the effects, extent and duration of the breach and mitigate harmful effects. These steps will vary depending on the precise nature, scale and severity of the breach and may include:

- making efforts to recover personal information if the breach involved such information
- securing, isolation, access restriction, or shutting down of breached systems
- collaborating with external cyber security authorities
- suspending activities that led to the data breach
- revoking or changing access credentials
- instigating additional physical security measures.

Standard measures to contain and mitigate the breach will be applied to all breaches. Extra measures will be added based on the level of risk determined in the data breach assessment. This assessment will be reviewed throughout the management process, and more actions will be taken if needed.

4.4 Assessment

When investigating a data breach, the QCA will assess relevant information and risks associated with the breach to determine next steps. This information will include:

- the date, time, duration and location of the breach
- how the breach was discovered, and who reported the breach
- the cause and extent of the breach
- the nature and sensitivity of information
- if any personal information is involved:
  - a list of affected individuals, or potentially affected individuals
  - the likelihood of serious harm occurring to affected individuals to whom the personal information relates, having regard to the matters listed in s. 47(2).

Where it is not immediately clear whether a data breach is an eligible data breach, but reasonable suspicion arises, the QCA will assess whether there are reasonable grounds to believe the data breach is an eligible data breach. This assessment will be documented and completed within 30 days (s. 48(3)) of the suspicion forming, unless an extended assessment period (s. 49) is required.

4.5 Notification

Where a data breach has been determined or is reasonably believed to be an eligible data breach, the QCA will notify the Information Commissioner (s. 51) and particular individuals (s. 53) as soon as practicable unless an exemption (ss. 55–60) applies.

Notification to the Information Commissioner

A statement including the information required in section 51(2) will be prepared and provided to the Information Commissioner when the QCA knows, or reasonably believes, an eligible data breach has occurred. This statement will be provided to the Office of the Information Commissioner (OIC) through its online reporting portal.

Notification to particular individuals

The QCA will follow the steps set out in section 53 to notify particular individuals and provide them with the information required in s. 53(2).

Depending on the circumstances, notifications will be made via the most reasonably practicable option under s. 53(1). The QCA will take one of the following steps:

(a) notify each individual whose personal information has been accessed, disclosed or lost
(b) notify each **affected** individual
(c) publish the information detailed in s. 53(2) on the QCA website for a period of at least 12 months, other than information that would prejudice the functions of the QCA.

Notifying other entities

Data breaches will be reported to the Queensland Government Cyber Security Unit (CSU) by the QCA as required under the information security incident reporting standard.[1]

Depending on the circumstances of the data breach and the categories of data involved, the QCA may also need to report to or engage with:

- Queensland Police Service
- Crime and Corruption Commission Queensland
- Queensland State Archives
- Office of the Australian Information Commissioner
- other entities as required by contract or other laws.

4.6 Post data breach review and remediation

After managing a data breach, the Crisis Management Team will review what happened to learn from it, make improvements and implement other remedial steps (where possible). The review will depend on how serious and widespread the breach was, but will include:

- gaining an understanding how the data breach was caused and what steps were taken to mitigate or eliminate the possibility of reoccurrence
- analysing how well existing breach measures worked to identify, contain and mitigate the impact of the breach
- reviewing other key learnings resulting from the data breach management process
- identifying any potential changes that should be made to prevent or reduce risk of reoccurrence. Changes that were agreed should be actioned promptly and key procedural changes communicated to staff
- ensuring an accurate record of the data breach is captured, maintained and reported as appropriate
- ensuring any eligible data breach has been recorded in the register by the Information Management Officer.

5. Eligible data breach register

As required under section 72 of the IP Act, the QCA will maintain a register detailing any eligible data breaches. This register will include the information required under section 72(2) (Box 2).

[1] Queensland Government, *Information security incident reporting standard*, Queensland Government website, September 2024, accessed 3 June 2025.

Box 2: Section 72(2) of the IP Act

(2) The register must include the following information for each eligible data breach–

(a) a description of the eligible data breach, including the type of data breach under section 47;
(b) if a statement is required for the eligible data breach under section 51–the date the statement is provided;
(c) if further information about the eligible data breach is required to be given to the information commissioner under section 52–each date the further information is given;
(d) if individuals are notified of the eligible data breach under section 53(1)(a) or (b)–the individuals notified and the date and method used to notify the individuals;
(e) if the agency relied on an exemption under part 3, division 3–the exemption relied on;
(f) details of the steps taken by the agency to–

i. contain the eligible data breach under section 48(2)(a) or (4)(a); and
ii. mitigate the harm caused by the eligible data breach under section 48(4)(a);

(g) details of the actions taken by the agency to prevent future data breaches of a similar kind occurring.

6. Related QCA documents

- Information Privacy Policy
- Security Incident Response Plan
- IT Disaster Recovery Plan
- Business Continuity Plan

Release notice

Version	Amendment details	Responsible officer	Date
1.0	New policy created	Information Management Officer	01/07/2025

Approved:

Flavio Menezes

Chair

1/07/2025

Approval and release date

1/07/2025

Planned review date

1/07/2026