

Data Breach Policy

CM Reference: DOC/26/53965 | **Version:** 2.0 | **Version effective:** 01/09/2026

Purpose

The purpose of this policy is to outline the approach the Queensland Reconstruction Agency (QRA) will undertake regarding its response to data breaches, the roles and responsibilities QRA maintains in relation to managing data breaches and to ensure compliance with the *Information Privacy Act 2009* (Qld) (IP Act) and the Queensland Government Information and Cyber Security Policy (IS18).

Scope

This policy applies:

- where any QRA held data is breached through human error, technical error or malicious action whereby an unauthorised person may gain access to the data.
- to all individuals employed or engaged by QRA, including but not limited to, permanent, temporary, casual and part-time employees, contractors, agency staff, volunteers and consultants.
- to all activities, operations and interactions undertaken in the course of performing duties for or on behalf of QRA, regardless of location. This includes activities conducted on QRA premises, during remote work, at off-site locations, and while using QRA resources or representing QRA in any capacity.

Policy statement

Reporting a breach

All QRA staff share a responsibility to safely handle information in our care, in line with the policies and standards of QRAs Information Security Management System (ISMS) and in line with the Queensland Privacy Principles (QPPs) detailed in the IP Act. Similarly, it is a responsibility of all staff to raise an alert where a breach is detected. This is done using the existing internal Support communication channels.

External parties can alert QRA to a potential breach via the info@qra.qld.gov.au email address.

Managing a breach

QRAs response to a data breach follows the approach of:

- Contain & mitigate the breach
- Assess the breach
- Notify affected individuals
- Review the event and plan for improvements

Containment is key to limit the spread of the breach and to limit its impact. In the initial stages of a breach, emphasis is on identifying what data is affected, the likely mechanism of how the breach occurred and for steps to be taken to close off or limit further breach actions.

In assessing the breach, in conjunction with the Information Security Officer, an analysis will be performed by the Privacy Officer of the nature of the breach, the factors relating to the data impacted and, within 30 days, an assessment of whether the breach constitutes an eligible data breach and therefore requires notification to be sent to the Office of the Information Commissioner (OIC).

Should an eligible data breach occur, the Privacy Officer will determine to what extent individuals are impacted and make recommendation of how best to notify them of the breach, and any containment or mitigation actions and potential risks to themselves. This notification will be developed in conjunction with QRAs Strategy and Engagement team to ensure the most appropriate method of communication for the specific breach is used.

It is the responsibility of the Information Security Officer to maintain a register of eligible breaches for future reporting and analysis.

Once the breach has been contained, assessed, and, in the case of an eligible breach, impacted individuals notified, a review by the Information Security Officer will occur to identify how such a breach can be prevented in future. In conjunction with other business units an action plan will be developed to address recommendations, and this plan will be monitored for progress by QRAs Executive Leadership Team.

Mandatory requirements

To meet the intent of this policy to act responsibly regarding the privacy of QRA held data and maintain compliance with the IP Act and QRAs broader Information Security Policy objectives:

- Staff must report suspected security incidents, including suspected data breaches.
- Managers and Directors must implement and maintain business practices with respect to the Queensland Privacy Principles (QPPs).
- Suspected data breaches must be assessed to determine if they are to be considered an Eligible Data Breach.
- Eligible data breaches must be responded to immediately, with reasonable steps taken to contain and mitigate the breach from causing harm.
- Notification of Eligible Data Breaches must be made to the OIC and affected individuals where required.
- A register of Eligible Data Breaches must be maintained.

Authority

[Information Privacy Act 2009 \(Qld\)](#)

Delegations

Nil

Roles and responsibilities

Role / Body	Responsibility
Chief Executive Officer (CEO)	Ensure QRA operates an Information Security Policy and ISMS in line with Queensland Government IS18 policy and meets its obligations regarding the IP Act.

Role / Body	Responsibility
Information Security Officer (ISO) (as delegated per QRAs Information Security Management Framework)	Investigate, assess and manage potential data breaches, notifying the Privacy Officer where they are confirmed to have occurred, maintain data breach registers and report to QRA leadership regularly. Act as the Incident Manager for any security related incident under QRAs Security Incident Management Response Plan. Manage the identification of an eligible data breach and any subsequent OIC engagement in the absence of the Privacy Officer.
Privacy Officer	Assess the privacy implications of data breaches, determining where eligible data breaches have occurred, advise the ISO of mandatory notification obligations and liaise with the OIC as required.
ICT Director	Assist the ISO with prioritised resourcing in relation to data breach investigation, mitigation and forensic collection.
QRA Managers, Directors and Executives	Establish and maintain working practices in line with QRAs ISMS and Information Security Policy and the IP Act. Provide resourcing and support to ongoing breach investigations.
QRA engaged suppliers/vendors	Maintain secure working practices in line with QRAs Information Security Policy and contracted obligations related to the IP Act.
All QRA Staff and Contractors	Maintain safe data handling practices in line with QRAs Information Security Policy and with regard to obligations under the IP Act. Notify any suspected data breaches via Support.

Related documents

The following related documents should be read in conjunction with this policy:

QRA Policies and Procedures

- Cyber Security Incident Response Plan
- Playbook – Data Breach
- [Privacy Policy](#)

Other References / Resources

- [Queensland Government Information and Cyber Security Policy \(IS18:2025\)](#)
- [Public Sector Act 2022 \(Qld\)](#)
- [Information Privacy Act 2009 \(Qld\)](#)
- [Human Rights Act 2019 \(Qld\)](#)

Definitions

Term	Definition
Data Breach	An event of unauthorised access to, disclosure of, or loss (including destruction of) QRA held data, potentially causing harm.
Eligible Data Breach	An “Eligible Data Breach” will have occurred under the IP Act where: - 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 - 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.
Serious Harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: - 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.
Mitigation	Action taken to minimise risk related to a breach, such as back-ups, encryption and other technical restrictions. May also relate to non-technical efforts to limit impact of a breach.
Unauthorised Access	Access to data by an individual or entity without permission. Examples include: - An employee browsing records without a legitimate purpose. - A cyberattack compromising QRA systems.
Unauthorised Disclosure	Disclosure of data to an unauthorised party. Examples include: - Sending personal information to the wrong recipient. - Publishing sensitive information online without consent.
ISMS	Information Security Management System, aligned to ISO27001, a collection of policies and procedures operated with the intent of managing information security risks across QRA.
QPP	Queensland Privacy Principles, detailed within the IP Act set out the requirements of organisations in relation to the holding, processing and management of personal information.

Review

The Chief Executive Officer will review this policy within twelve months of the initial approval date, then at least once every three years, and as required to consider changes to relevant legislation, government policy and practices, changing trends, and feedback.

Document control

Version no.	Date	Approved by	Next scheduled review date
1	June 2025	Major General Jake Ellwood (Rtd), CEO	July 2026
2	1 September 2026	Major General Jake Ellwood (Rtd), CEO	September 2029

Contact

For further information, please contact:

Queensland Reconstruction Authority

Email: info@gra.qld.gov.au