

# Data Breach Policy

Effective Date:	7 August 2025	Version	1.0
Review Date:	7 August 2028		
Policy Owner:	Executive Manager, Corporate Governance and Performance		
Policy Approval Delegate:	Chief Executive Officer		

## Contents

<b>1</b>	Policy Statement .....	<b>3</b>
<b>2</b>	Purpose.....	<b>3</b>
<b>3</b>	Principles .....	<b>3</b>
3.1	Addressing a data breach.....	3
3.2	Review .....	3
3.3	Notification and reporting.....	4
<b>4</b>	Scope.....	<b>4</b>
<b>5</b>	Context.....	<b>4</b>
<b>6</b>	Responsibilities .....	<b>5</b>
6.1	Chief Executive Officer .....	5
6.2	Executive Leadership Team.....	5
6.3	Senior Managers and Managers.....	5
6.4	Executive Manager, Corporate Governance and Performance .....	5
6.5	Senior Manager, Technology and Business Information.....	6
6.6	Manager, Marketing and Communication.....	6
6.7	Employees.....	6
<b>7</b>	Procedure .....	<b>7</b>
7.1	Addressing suspected data breach.....	7
7.2	Reviewing a data breach .....	7
7.3	Reporting and proactive management.....	7
<b>8</b>	<i>Human Rights Act 2019 (Qld)</i> .....	<b>8</b>
<b>9</b>	Glossary.....	<b>8</b>
<b>10</b>	Legislative Context.....	<b>8</b>
<b>11</b>	Associated Documentation.....	<b>9</b>



**Queensland Rural and Industry Development Authority**

---

**12** References..... 9

**13** Executive Endorsement..... 9

**14** Version History ..... 9

## Queensland Rural and Industry Development Authority

---

### 1 Policy Statement

The Queensland Rural and Industry Development Authority (QRIDA) is responsible under the *Information Privacy Act 2009* (Qld) (IP Act) to proactively respond to: unauthorised access to; disclosure of; or loss of personal information held by the organisation, and to investigate these breaches to prevent or reduce the risk of reoccurrence.

### 2 Purpose

The Data Breach Policy establishes QRIDA's obligations and responsibilities to investigate, control, and mitigate instances of unauthorised access to, or disclosure of, personal information held by the organisation and, if identified, to report eligible data breaches to the Office of the Information Commissioner (OIC) under the Mandatory Notification of Data Breach Scheme (MNDBS) (Chapter 3A of the IP Act).

### 3 Principles

A *data breach* is the unauthorised access to, or disclosure of, information held by an organisation, regardless of whether the information is:

- held physically or digitally
- accessed or disclosed intentionally or accidentally.

#### 3.1 Addressing a data breach

QRIDA will work to contain and mitigate data breaches:

- immediately upon becoming aware of the data breach
- in coordination with other business units once reported to the Corporate Governance and Policy (CGP) business unit until no further action is possible.

All data breaches are reported to CGP, logged in the Data Breach Register and assessed for severity. The severity of data breaches must be assessed with consideration to:

- the type of information (personal, sensitive, or neither, as defined by the IP Act)
- the party/ies that accessed the information or had it disclosed to them (within the organisation, between the organisation and another agency bound by the IP act, or outside the organisation)
- controls in place that may limit or prevent access to the information
- the harm that may be caused by the information being accessed or disclosed.

#### 3.2 Review

Following the addressing of a data breach, QRIDA will undertake a review process to determine the cause of the breach. This will give consideration to whether the breach was a result of:

- information technology (IT) vulnerability: that is, whether IT systems are configured in such a way that the data breach is likely to reoccur
- process failure: that is, whether the data breach was a result of insufficient rigour around business processes and therefore, could have occurred by any employee acting in good faith

## Queensland Rural and Industry Development Authority

---

- individual action: that is, whether the data breach was a result of the actions of an individual, either through human error, incompetence or intentional disregard for processes
- a combination of identified factors.

Once the cause(s) of the data breach has/have been identified, QRIDA will work to rectify the issue(s) to reduce the risk of reoccurrence.

### 3.3 Notification and reporting

An eligible data breach must be reported to the Information Commissioner under the MNDBS if CGP:

- identifies that the data breach involved personal information; and
- determines it is likely (i.e. more probable than not) to result in serious harm to an individual whose information was involved in the breach.

Where an eligible data breach occurs, QRIDA will notify OIC and impacted individuals either through individual notification or publishing a notice on the QRIDA website that includes:

- the date on which the breach occurred, if known
- a description of the data breach
- an explanation of how the data breach occurred
- the steps QRIDA has taken to contain and mitigate the breach
- recommendations on steps individuals should take in response to the data breach
- contact information for QRIDA, including information on how to make a privacy complaint
- other agencies involved in the data breach, if applicable
- if the data breach involved unauthorised access or disclosure: the period over which access or disclosure was made (i.e. the period of time that the data was accessible).

QRIDA will also, at the discretion of the Executive Manager, Corporate Governance and Performance (EM-CGP) voluntarily report data breaches considered of significant risk to OIC and impacted individuals, regardless of eligibility under the MNDBS.

## 4 Scope

The Data Breach Policy encompasses QRIDA's obligations and responsibilities in the event of a data breach:

- requests for the authorised release of information are managed under the Access to Information Framework
- obligations and responsibilities in the management of information (the implementation of which is intended to prevent data breaches) are under the Information Management Framework.

## 5 Context

The *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (IPOLA Act) introduced the MNDBS from 1 July 2025. When a data breach occurs, or is suspected to have occurred, agencies must:

- take all reasonable steps to contain and mitigate data breaches

## Queensland Rural and Industry Development Authority

---

- assess within 30 days whether the breach is an *eligible data breach* and, if so, notify the Information Commissioner and particular individuals
- prepare and publish a data breach policy detailing how it will respond to data breaches and suspected data breaches
- keep a register of eligible data breaches.

QRIDA has an Averse risk appetite concerning the security of confidential and personal information and malicious cyber activity. Consequently, and to support its commitment to continuous improvement, QRIDA has adopted a broader approach to the management of data breaches than the requirements of the MNDBS to:

- prioritise the identification and management of all data breaches
- allow employees and managers involved in a data breach to focus on containment and mitigation within their area of responsibility
- establish clear separation of responsibilities between those involved in the data breach and those investigating and assessing it
- reduce the risk of eligible data breaches occurring by engaging in a process of continuous improvement.

## 6 Responsibilities

### 6.1 Chief Executive Officer

The Chief Executive Officer (CEO) is responsible for:

- (a) approving this Policy and supporting its implementation throughout the organisation
- (b) negotiating with other agencies to determine responsibility for undertaking notification under the MNDBS.

### 6.2 Executive Leadership Team

The Executive Leadership Team (ELT) is responsible for:

- (a) supporting the implementation of this Policy throughout the organisation.

### 6.3 Senior Managers and Managers

The QRIDA Senior Managers and Managers are responsible for:

- (a) informing employees under their supervision or management of this Policy and ensuring it is complied with on an ongoing basis
- (b) taking immediate action to contain and mitigate data breaches when they occur
- (c) reporting data breaches to CGP within one business day of being identified or suspected.
- (d) supporting CGP in the investigation of data breaches.

### 6.4 Executive Manager, Corporate Governance and Performance

The EM-CGP is responsible for:

- (a) reviewing this Policy triennially to ensure it remains current
- (b) recommending amendments to this Policy as required
- (c) preparing and making available resources and training for:
  - i. staff to understand their duties and responsibilities in relation to this policy

## Queensland Rural and Industry Development Authority

---

- ii. employees responsible for the assessment of data breaches in alignment with OIC guidance.
- (d) arranging publication of this Policy on the QRIDA public-facing website
- (e) maintaining the Data Breach Register, including logging incidents reported by the Technology and Business Information (TBI) business unit, updating incident records when new information is available, and extracting and providing records when requested
- (f) oversight of data breach assessments and implementation of an action plan to control and mitigate breaches when they occur, are suspected to have occurred, or is likely to occur
- (g) oversight of eligible data breach submissions to the OIC under the MNDBS
- (h) if an eligible data breach is deemed to have occurred, workflow management of plans developed in consultation with the Marketing and Communications (M&C) and Client Engagement (CE) business units to notify individuals impacted by the data breach
- (i) oversight of investigations into data breaches once they have been contained to identify the cause(s) of the breach
- (j) implementing organisational training and changes to policies, procedures, business processes and systems to prevent or reduce the risk of occurrence of data breaches.

### 6.5 Senior Manager, Technology and Business Information

The Senior Manager, Technology and Business Information (SM-TBI) is responsible for:

- (a) supporting CGP in the investigation of data breaches where an IT vulnerability is identified
- (b) recommending amendments to this Policy as required
- (c) implementing changes to TBI policies and procedures to prevent or reduce the likelihood of the occurrence of data breaches
- (d) recommending changes to business practices outside to prevent or reduce the likelihood of the occurrence of data breaches.

### 6.6 Manager, Marketing and Communication

The Manager, Marketing and Communication is responsible for:

- (a) making this policy available on the QRIDA website
- (b) developing supporting documentation (e.g. data breach notice for distribution to impacted individuals) in consultation with CGP
- (c) if requested by CGP, publishing information about eligible data breaches on the QRIDA website for a period of at least 12 months.

### 6.7 Employees

QRIDA employees are responsible for:

- (a) familiarising themselves with the requirements of this Policy
- (b) acting in accordance with this Policy and the QRIDA Code of Conduct
- (c) taking immediate action to contain and mitigate data breaches when they occur within the scope of their role responsibilities

## Queensland Rural and Industry Development Authority

---

- (d) notifying their manager or, in the absence of their immediate manager, the Senior Manager of their business unit or division, when a data breach occurs, is suspected to have occurred, or is likely to occur
- (e) supporting their manager and/or CGP in the investigation of data breaches.

### 7 Procedure

Detailed organisational procedures for the management of data breaches are developed and implemented by the CGP business unit, ensuring they incorporate the principles of this Policy.

#### 7.1 Addressing suspected data breach

- (a) As soon as a suspected data breach is identified, employees must take measures to contain and mitigate the breach, then notify their manager as soon as practicable.
- (b) If additional measures can be taken to contain the mitigate the breach, managers should action these prior to advising CGP of the breach, within one business day.
- (c) CGP will assess the data breach to determine information and individuals impacted.
- (d) If the involvement of another agency is identified, the breach will be escalated to the CEO for negotiations with that agency to determine whether QRIDA will act as the lead. Should the other agency be identified as the lead agency, QRIDA holds no further action.
- (e) Where QRIDA is the only agency identified, CGP will manage any additional containment or mitigation actions, in addition to logging the breach in the Data Breach Register and the development and implementation of a notification plan to inform those impacted by the breach, with CEO approval where necessary.

#### 7.2 Reviewing a data breach

- (a) Once no further action can be taken to mitigate or contain the data breach, and within the 30-day period following awareness of the data breach, CGP will investigate the underlying causes of the breach.
- (b) From the results of this investigation, CGP will arrange or make recommendations for action within the appropriate business unit.
- (c) Following the completion of any action, CGP will reassess to determine the likelihood of breach reoccurrence.

#### 7.3 Reporting and proactive management

- (a) Due to the sensitivity of the information recorded therein, access to the Data Breach Register will be restricted to employees who require access as part of their role responsibilities.
- (b) CGP will develop reporting that enables organisational and managerial oversight of data breaches for the ELT, including a monthly Breach Report provided to the CEO.
- (c) Following review, or within 30 days of being made aware of the potential data breach, whichever is earlier, CGP will:
  - i. determine whether it is an eligible data breach under the MNDBS or if it is a non-eligible breach that warrants voluntary disclosure
  - ii. submit information about the breach to the OIC or request an extension within that same period.

## Queensland Rural and Industry Development Authority

### 8 *Human Rights Act 2019 (Qld)*

QRIDA is committed to respecting, protecting and promoting human rights. Under the *Human Rights Act 2019 (Qld)*, QRIDA has an obligation to act and make decisions in a way that is compatible with human rights, and when making a decision, to give proper consideration to human rights. When making a decision about this policy and procedure, decision makers must comply with that obligation.

### 9 Glossary

Term	Definition
Chief Executive Officer (CEO)	Chief Executive Officer of QRIDA.
Code of Conduct	QRIDA Code of Conduct.
Data	Any information held by QRIDA, including both physical and digital records.
Data breach	Either of the following in relation to information held by QRIDA: (a) unauthorised access to, or unauthorised disclosure of, the information; (b) the loss of the information in circumstances where unauthorised access to, or unauthorised access of, the information is likely to occur.
Eligible data breach	Refer Chapter 3A, Part 1, Section 47 of the IP Act.
Employee	For the purposes of this document, employee includes permanent, temporary and casual employees, contractors, consultants, students, volunteers and others who exercise power or control resources for or on behalf of QRIDA.
Executive Leadership Team (ELT)	<ul style="list-style-type: none"> <li>• Chief Executive Officer</li> <li>• Chief Operating Officer</li> <li>• Chief Lending Officer</li> <li>• Chief Engagement Officer</li> </ul>
Manager	An employee of QRIDA who is in charge of a QRIDA business unit and has staff reporting to him/her/them and exercises a financial or human resource delegation in accordance with QRIDA's Financial Delegations Schedule or Human Resources Delegations Schedule.

### 10 Legislative Context

- (a) [\*Rural and Regional Adjustment Act 1994 \(Qld\)\*](#)
- (b) [\*Rural and Regional Adjustment Regulation 2011 \(Qld\)\*](#)
- (c) [\*Statutory Bodies Financial Arrangements Act 1982 \(Qld\)\*](#)
- (d) [\*Human Rights Act 2019 \(Qld\)\*](#)



## Queensland Rural and Industry Development Authority

- (e) [Public Sector Act 2022 \(Qld\)](#)
- (f) [Information Privacy Act 2009 \(Qld\)](#)
- (g) [Privacy Act 1988 \(Cth\)](#)


### 11 Associated Documentation

- (a) [QRIDA Code of Conduct](#)

### 12 References

- (a) OIC (August 2024). [IPOLA Guideline: Mandatory Notification of Data Breach scheme.](#)
- (b) [OIC MNDB Assessment Tool](#)

### 13 Executive Endorsement

<b>Name</b> Cameron MacMillan	<b>Position</b> Chief Executive Officer
<b>Signature</b> 	<b>Date</b> 7 August 2025

### 14 Version History

Date	Version	Review
July 2025	1.0	Formation of new Policy in accordance with legislative requirements under the <i>Information Privacy and Other Legislation Amendment Act 2023</i> .