OFFICE OF THE QUEENSLAND Integrity Commissioner

POLICY

Data Breach

Version: 1.0| Version effective: 26/06/2025

Audience

Internal

Function area

Corporate

Purpose

This policy outlines the principles the Office of the Queensland Integrity Commissioner (OQIC) will follow for identifying, assessing, reporting and responding to data breaches and eligible data breaches under the *Information Privacy Act 2009*.

Policy statement

This policy complies with section 73 of the *Information Privacy Act 2009* and outlines the OQIC's overall strategy for managing eligible data breaches in line with the Mandatory Notification of Data Breach scheme (MNDB scheme).

As required by the MNDB scheme, the OQIC will:

- publish and maintain policies and procedures to manage data breaches involving personal information, and
- notify the Information Commissioner and affected individuals of an eligible data breach (unless an exemption to notification applies).

This policy should be read in conjunction with the OQIC Data Breach Response Plan.

Key terms used in this policy are explained in the definitions section towards the end.

Principles

Principle	What this means for OQIC
Transparency	Promptly inform individuals if their personal information has been compromised, ensuring they are aware and can take protective action.
Accountability	Take responsibility to safeguard personal information and respond effectively and appropriately in a timely manner.
Assessment	Assess the severity and determine the likelihood of serious harm when determining the appropriate course of action.
Protective	Take all reasonable steps to prevent a data breach from occurring, but if it does, review and strengthen policies, procedures and systems to prevent further incidents.

Principle	What this means for OQIC
Confidentiality	Ensure all notifications and responses respect the privacy of individuals and do not expose further personal or sensitive information.

Requirements

The OQIC takes data breaches seriously and works to minimise risks to security and use of data. All OQIC staff are required to play a part in identifying, reporting and preventing data breaches.

1. Compliance with the MNDB scheme

The OQIC complies with the MNDB scheme and will respond to a known or suspected eligible data breach by:

- immediately taking all reasonable steps to contain and mitigate the data breach
- assessing the suspected data breach within 30 days (unless an extension is required) to determine if there are reasonable grounds to believe a data breach is an eligible data breach under the MNDB scheme
- notifying any other affected agencies
- notifying the Information Commissioner and any affected individuals where there are reasonable grounds to believe an eligible data breach has occurred unless an exemption to notification applies.

2. Working with others

The OQIC works closely with external service providers in managing data and reviewing the controls. Risk assessment is undertaken before engaging any new provider involved in managing or storing data on behalf of the OQIC.

The OQIC also collaborates with other government agencies to align with Queensland Government information security reporting and incident response protocols.

3. Identifying and reporting breaches

As prompt detection of data breaches improves the ability to contain the breach and mitigate potential harm, OQIC encourages staff and external entities to report known or suspected data breaches as soon as possible.

OQIC staff are equipped to identify data breaches through internal training and awareness. OQIC staff can report actual or suspected data breaches to the Data Breach Response Coordinator or any member of the Executive Leadership Team (ELT).

Information is provided on the OQIC website on how external entities can report known or suspected data breaches to the OQIC.

4. Data breach response plan

The OQIC's Data Breach Response Plan outlines the approach taken by the OQIC to identify and manage data breaches, including known or suspected eligible data breaches.

This operational procedure document outlines the steps OQIC takes in responding to data breaches to contain and mitigate harm, assess a data breach, notify relevant parties and prevent data breaches.

The Data Breach Response Plan also outlines:

- roles and responsibilities related to identifying, reporting, containing, mitigating, assessing and preventing data breaches

- the notification strategy to enable quick and effective communication with affected individuals and the Information Commissioner
- instances where external reporting or engagement may be necessary
- schedule for testing and reviewing the response process.

5. Authorised roles

As the officer responsible for the OQIC, the Integrity Commissioner is the decision-maker relating to the *Information Privacy Act 2009*, including deciding if a data breach is an eligible data breach under the MNDB scheme.

While the Integrity Commissioner may direct or authorise anyone to undertake actions in assessing and responding to a data breach, the following roles are authorised under this policy:

Role	**Responsibilities**	**Officer**
Data Breach Response Coordinator	• receive and assess all reported breaches • lead the Data Breach Response Team • seek an extension from the Information Commissioner where required • principal contact regarding MNDB scheme • engage with other agencies as required • engage with third-party providers to establish a shared responsibility model for responding to data breaches • manage and maintain the OQIC's Eligible Data Breach Register and associated records.	Manager, Corporate Services or any other role authorised by the Integrity Commissioner
Data Breach Response Team	• contain any known or suspected eligible data breach and implement mitigation strategies • oversee formal assessment of suspected eligible data breaches is undertaken • ensure post review is undertaken and recommendations are provided to decision-maker for consideration.	OQIC Executive Leadership Team (ELT) members, plus Strategic IT and Digital Systems Manager

6. Recordkeeping and review

The OQIC will maintain all records related to compliance with the MNDB scheme securely and in accordance with the OQIC's recording keeping policies and the *Public Records Act 2003*.

All details of eligible data breaches are recorded in the OQIC's Eligible Data Breach Register.

The OQIC will conduct periodic reviews of data incidents and breaches to monitor, analyse and review the type and severity of data breaches, along with the effectiveness of response methods. Along with the schedule for testing and review, the Data Breach Response Plan also provides guidance on post-response assessments to inform continual improvement.

Definitions

Term	Definition
Affected individual	An individual is considered an affected individual if the unauthorised access, disclosure or loss of their personal information is likely to result in serious harm to them.
Data breach	When information held by the OQIC is subject to unauthorised access, disclosure or is lost and the loss is likely to result in unauthorised access or disclosure.
Eligible data breach	Section 47 of the *Information Privacy Act 2009* defines an eligible data breach of an agency occurring when 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.
MNDB scheme	As defined in Part 3A of the *Information Privacy Act 2009*.
OQIC staff	All OQIC permanent full time, part time, permanent and temporary staff authorised to access OQIC information systems and assets. Any consultants and persons or organisations authorised to administer, develop, manage and support OQIC information systems and assets.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion – • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not.

Serious harm	Schedule 5 of the *Information Privacy Act 2009* defines serious harm as being to an individual in relation to the unauthorised access or disclosure of the individual's personal information, including 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.
Suspected eligible data breach	Occurs when there is a reasonable suspicion that an eligible data breach has occurred, but further investigation is required to confirm.

Legislation

- *Information Privacy Act 2009*
- *Integrity Act 2009*
- *Public Records Act 2023*

Delegations/Authorisations

- OQIC Data Breach Policy (this document)

Policies and procedures in this group

- OQIC Data Breach Response Plan
- OQIC Privacy Policy
- OQIC Eligible Data Breach Register

Supporting information for this policy

- IPOLA Guidelines | Office of the Information Commissioner Queensland

Other resources

- Queensland Treasury, A Guide to Risk Management
- Business continuity management and ICT disaster recovery implementation fact sheet
- Responding to and recovering from cyber-attacks – Queensland Audit Office

Key data

Item	**Note/relevant information**	**As at [date]**
Document owner	Manager, Corporate Services	26/06/2025
TRIM reference	QIC/25/4247	26/06/2025
Review period	3 years	26/06/2028
Keywords	MNDB, Mandatory notification of data breach, data breach, privacy principles, data breach register, personal information	

Document history

Date	Version number	Author	Description of changes
22/04/2025	1.0	Ruth May	Initial draft
11/06/2025	1.0	Monique Brown	Review of initial draft
13/06/2025	1.0	Cyrilla Eastwood	Review of policy draft

Approval

Role	Name	Position	Date
Approver	Paxton Booth	Acting Integrity Commissioner	26/06/2025