**Applying the legislation –**

***Information Privacy Act 2009***

**TEMPLATE**

DATA BREACH RESPONSE PLAN TEMPLATE

# Introduction

From 1 July 2025, a Mandatory Notification of Data Breach (**MNDB**) scheme will apply to Queensland public sector agencies that are subject to the *Information Privacy Act 2009* (Qld) (**IP Act**). From 1 July 2026, the MNDB scheme will apply to local government.

The MNDB scheme requires agencies to take prescribed actions where an agency knows or reasonably suspects that a data breach is an ‘Eligible Data Breach’. Agencies must:

* immediately take all reasonable steps to contain and mitigate the data breach. If the agency does not know if the data breach is an ‘Eligible Data Breach’, it must assess, within 30 days, and
* notify other affected agencies, and, if the agency knows or assess the data breach as an ‘Eligible Data Breach’, notify the Office of the Information Commissioner (**OIC**) and individuals whose personal information is the subject of the data breach, unless an exemption to notification applies.

To comply with the MNDB scheme, agencies need to prepare and publish a **Data Breach Policy** which is required under section 73 of the IP Act to detail how an agency will respond to data breaches.

# What is a Data Breach Response Plan?

While the preparation of a **Data Breach Response Plan** is not a mandatory requirement under the IP Act, it supports agency compliance and is considered good practice in responding to data breaches. A **Data Breach Response Plan** must align with the agency's associated **Data Breach Policy** and **Register of Eligible Data Breaches**, which are required under the IP Act.

A **Data Breach Response Plan** specifies, by way of practical, step by step detail, what an agency will do in responding to a data breach, with reference to the specific needs, systems and processes that are in place in an agency. It supports and expands on a **Data Breach Policy which** outlines an agency’s overarching policy in responding to data breaches, including 'Suspected Eligible Data Breaches'.

# Data Breach Response Plan Template

To assist agencies to develop a **Data Breach Response Plan**, the OIC has designed the **Data Breach Response Plan Template**.

A **Data Breach Response Plan**, while providing practical guidance and assistance, also needs to be flexible as not all data breaches will be the same. There is no 'one-size fit all' approach in the design of this kind of document.

The remainder of this document includes:

* commentary on the steps that may be included in a **Data Breach Response Plan** and the kind of information that may be included in each step, and
* the **Data Breach Response Plan Template.**

The structure of the commentary follows the six distinct stages used in the **Data Breach Policy**:

**Stage 1** – Preparation

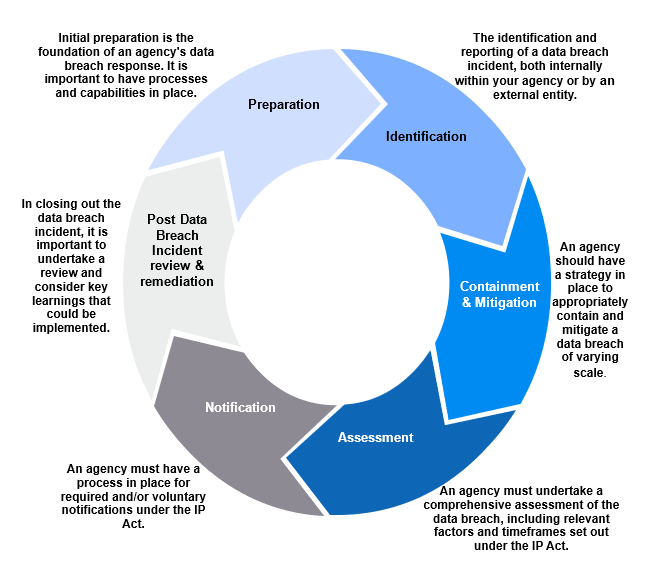
**Stage 2** – Identification

**Stage 3** – Containment & mitigation

**Stage 4** – Assessment

**Stage 5** – Notification

**Stage 6** – Post-data breach incident review & remediation



In practice, agencies may need to undertake some of these stages concurrently when responding to a data breach. However, for ease of accessibility, it is recommended that a response plan adopts a "step by step" approach for each stage in responding to data breaches.

Additionally, the scale and scope of the activities that an agency may take will depend on the agency in question, noting varied levels of complexity, resources, expertise and experience in responding to data breaches.

**Undertaking an appropriate level of preparatory actions to support agency readiness to respond to data breaches is a critical first component.**

While the nature and scope of systems, processes and procedures, and resources will vary across agencies, there are some key activities and actions that can be taken in preparing to respond to data breaches or suspected data breaches.

In this stage an agency should identify the range of systems, processes, procedures and resources that are in place to respond to a data breach or suspected data breach.The Data Breach Response Plan may act as a checklist or expand on the Data Breach Policy in the following areas:

* ensuring appropriate policies, procedures and systems are in place to identify data breaches and report them appropriately
* ensuring policies and procedures are in place for responding to data breaches, including how to undertake a data breach assessment with appropriate risk assessment, notification, and interconnected policies and procedures such as an agency cyber incident response plan, information security policy, notification and communication procedures
* identifying specific reporting lines, internal bodies decision-makers and escalation points attached to controls and other mechanisms used to identify data breaches and respond to data breaches. This should include the key reporting roles and responsibilities in a data breach response and identify any specific internal committee or body, such as a Data Breach Response Team, to be established as part of the data breach response process
* identifying specific roles and positions, including those making up the Data Breach Response Team, and how these may vary depending on the type or severity of a data breach. Depending on the type of breach, this Team may include representatives from the agency's IT, cybersecurity, communications, HR, Legal, Senior Executive, and Privacy teams. Subject matter experts may also need to be stood up depending on the source and nature of the data breach. Each member should be allocated responsibilities (e.g. making escalation decisions, reporting obligations, maintaining, testing, and updating the Data Breach Policy, data breach recordkeeping, and post-data-breach review and evaluation), and
* ensuring there is a broad awareness across the agency of the policies, procedures and obligations in place.

**A robust data breach response will effectively activate appropriate mechanisms, including policies, procedures, other controls and associated systems, to ensure that a data breach is detected and managed appropriately at this stage.**

It will be necessary for an agency, on identification of a data breach incident, to activate the necessary systems, processes and procedures in place to respond to a data breach or suspected data breach at the identification stage.

A Data Breach Response Plan should consider the following information and associated steps:

* requirements to activate an agency's data breach policy and response plan, and other relevant policies and processes such as cyber incident processes or information security requirements
* activating the agency's decision-makers and officers with specific roles and responsibilities in relation to data breaches. This may include convening an internal body such as the Data Breach Response Team with roles and responsibilities likely to vary dependant on the nature and seriousness of the data breach
* specifying the risk assessment parameters to categorise the breach in accordance with an agency’s risk management framework. A preliminary assessment should incorporate an initial rating of the data breach (e.g. low, medium or high risk) based on relevant factors including the nature of the data breach incident (i.e. internal or external causes), the nature of the information and the known scale of the data breach, and
* identifying appropriate escalation, resourcing and communication processes to adopt, based on the breach categorisation. For example, a breach rated as low risk may be dealt with by an agency's IT area whereas a breach rated medium to high risk may be escalated to officers including IT officers, the Privacy Officer and legal counsel.

**Containing and mitigating the data breach and the impacts of the data breach is a key focus of a data breach response plan.**

Agencies should consider containment methods proportionate to the size and scale of their agency and the type of information it collects, noting that what is reasonable will depend on the circumstances of the data breach.

A Data Breach Response Plan should consider the following information and associated steps:

* details of the agency's policies and procedures and specific controls that apply and should be considered in the mitigation and containment of the data breach
* the specific actions required to understand, on a preliminary basis, what has occurred in terms of the nature and scope of the data breach and the roles and responsibilities necessary to support this. This may include preliminary risk assessments that will frame the most appropriate containment and mitigation measures
* a requirement, where necessary, to obtain advice from agency and external experts to assist in understanding the nature of the data breach as well as the likely impacts and potential mitigation and containment strategies that could be engaged, and
* the key steps an agency should take in containing and mitigating the data breach, noting that this will vary dependant on the data breach.

**The IP Act imposes specific obligations for certain types of data breaches. It is therefore necessary to assess a data breach against the criteria prescribed under the IP Act to determine if the data breach is an Eligible Data Breach.**

In the Assessment stage, a Data Breach Response Plan may expand on the Data Breach Policy to provide greater detail in the following areas:

* the steps to be taken in an agency to consider the threshold tests under the IP Act that will determine whether the data breach is an Eligible Data Breach or a Suspected Eligible Data Breach
* details of how an agency will conduct a risk assessment to determine whether a data breach gives rise to serious harm to an individual
* identifying who, whether an officer or an internal board or committee, has responsibility for making the assessment decision
* identifying and explaining the escalation points for internal briefing purposes determining whether the assessment decision should be briefed to, for example, the agency CEO or Portfolio Minister
* prompting consideration of other issues that may be related to the assessment decision including:
* an agency’s contractual position with respect to any contracted service provider, and
* any legal or regulatory issues that may arise from the data breach.

**Subject to the outcome of the assessment of the data breach under the IP Act, an agency may be required to notify the Information Commission, affected individuals and/or other agencies.**

In the Notification stage, a Data Breach Response Plan may expand on the Data Breach Policy to provide greater detail in the following areas:

* identifying the specific decision-maker/s for notification decisions
* the roles and actions necessary to apply the agency's policies and procedures to assist in:
* determining whether the data breach requires notification and whether any exemptions from notification requirements are appropriate to engage
* identifying who has responsibility for making the notification to the Information Commissioner and any parties who should be consulted in making any notification
* identifying who has responsibility for making the notification to affected individuals and any parties who should be consulted in making any notification
* preparing a communications strategy for notifications and general external communications about the data breach.
* preparing for privacy complaints that may arise as a result of notification to affected individuals by outlining the approach to responding to complaints, for example, by developing a complaint response strategy for privacy complaints
* determining the level of detail to be included in the Eligible Data Breach Register (refer to the OIC's **Eligible Data Breach Register Template)**, and
* providing a prompt to assure consideration of other notification obligations engaged by the data breach – for example, Tax File Numbers under the *Privacy Act 1988* (Cth), corrupt conduct under the *Crime and Corruption Act 2001* (Qld), and the Queensland Police Service if criminal conduct is involved.

**It is important to undertake a post-incident review and remediation process to ensure key learnings are identified, and (where possible) improvements and other remediation activities implemented.**

In the post incident stage, a Data Breach Response Plan may expand on the Data Breach Policy to provide greater detail in the following areas:

* identifying the key officers or internal bodies responsible for overseeing the review and remediation process
* specific remediation activities required for different kinds of breaches (for example, this may include the steps required to resolve the incident, the reasonableness of what happened, what changes/controls will prevent or reduce risk of reoccurrence and the associated costs)
* assuring prompt consideration of other relevant legal and commercial issues, including liability, compensation, insurance, and other legal and regulatory issues, such as human rights that should be considered in the review and remediation process
* how the outcome of the review and remediation process should be detailed and escalated
* providing a process and actions for implementing recommendations of a review and remediation process, and
* prompting the agency to revisit and complete the Eligible Data Breach Register, if relevant (refer to the OIC's **Eligible Data Breach Register Template**).

# Data Breach Response Plan Template

This Template may be used by agencies subject to the MNDB scheme (noting the delayed commencement for local governments) including:

|  |  |  |  |
| --- | --- | --- | --- |
| Departments | Ministers | Public Authorities | Local Governments |

This Template should be read in conjunction with other guidance provided by the OIC. It is a general guide only and does not constitute legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, agencies should seek their own legal advice.

|  |
| --- |
| **For information and assistance on legislation, please refer to the appropriate Guidelines on OIC’s website, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au** |

Data Breach Response Plan Template

1. **Purpose and Scope**

*This section may consider:*

* *an overview of why a Data Breach Response Plan is important*
* *why the agency has the Data Breach Response Plan*
* *a high-level overview of what is included in the Data Breach Response Plan (e.g. the 6 stages in a response), and*
* *how the Data Breach Policy and Response Plan fits in within the agency's internal and external documents, including any other privacy and cyber policies.*

1. **Definitions**

*This may include any defined terms used through the Data Breach Response Plan. Defined terms should be consistent with the Data Breach Policy.*

1. **Roles and Responsibilities**

*This may include any defined terms used through the Data Breach Response Plan. Defined terms should be consistent with the Data Breach Policy.*

1. **Responding to a data breach**
   1. **Stage 1: Preparation**
   2. **Stage 2: Identification**

*An example of an internal reporting mechanism may include:*

|  |
| --- |
| *If an Agency Worker suspects there has been a data breach, they will immediately contact the [Privacy Officer or officer with responsibility for privacy compliance] and provide all relevant information. The [Privacy Officer will then conduct an immediate risk assessment of the breach.*   1. *If appropriate, the [Privacy Officer] will then escalate the matter so the Data Breach Response Team can be established. The Data Breach Response Team will establish a proactive and reactive communication strategy and consider the appropriateness of any immediate notifications. The agency will also consider engaging other internal teams to assist with managing the data breach (for example, legal counsel, senior management, media and communications, information security and human resources).* |

* 1. **Stage 3: Containment and Mitigation**
  2. **Stage 4: Assessment**

1. 1. **Stage 5: Notification**
   2. **Stage 6: Post-data-breach review and remediation**
2. **Record keeping**

*A Data Breach Response Plan may explain the agency's processes for documenting the management and response to data breaches and suspected data breaches.*

1. **Related Legislation and Policies**

*The Data Breach Response Plan will be developed alongside the Data Breach Policy. Any related relevant policies or legislation could be referenced here.*