**Applying the legislation –**

***Information Privacy Act 2009***

**TEMPLATE**

**DATA BREACH POLICY TEMPLATE**

# **Introduction**

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

The MNDB scheme requires agencies to take the following prescribed actions in responding to a data breach, including an ‘Eligible Data Breach’:

* 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, whether there are reasonable grounds to believe that the data breach is an ‘Eligible Data Breach’
* notify other affected agencies, and
* if the agency knows or assesses the data breach as an ‘Eligible Data Breach’, notify the Office of the Information Commissioner (**OIC**) and any individuals whose personal information is the subject of the data breach, unless an exemption to notification applies.

The MNDB scheme also requires agencies to prepare and publish a Data Breach Policy.

# **Data Breach Policy Template**

To assist agencies in complying with the MNDB scheme, the OIC has prepared this **Data Breach Policy Template** and the **Data Breach Response Plan Template.**

Although these Templates are **both** about how an agency responds to a data breach, a **Data Breach Policy** is intended to set out, at an overarching, policy level, how an agency will respond to a data breach while a **Data Breach Response Plan** sets out, on a step by step practical basis, how an agency will respond to a data breach.

Therefore:

* this **Data Breach** **Policy Template** is designed to assist agencies to develop a policy which outlines an agency’s overarching policy in responding to data breaches, including 'Suspected Eligible Data Breaches', and
* the **Data Breach** **Response Plan Template** is designed to assist agencies in preparing a step by step, practical plan for responding to an actual data breach, including 'Suspected Eligible Data Breaches' in accordance with the IP Act and best practice.

This **Data Breach Policy Template** includes commentary in relation to the necessary content of the Data Breach Policy under the IP Act and reflecting the commentary, a template Data Breach Policy.

# **What is a Data Breach Policy?**

Section 73 of the IP Act requires agencies to prepare, and publish on an accessible agency website, a Data Breach Policy detailing how an agency will respond to a data breach including data breaches that are **Eligible Data Breaches** or a **Suspected Eligible Data Breach**.

# **What is a data breach and an Eligible Data Breach under the IP Act?**

A **data breach** is defined in the IP Act to mean the unauthorised access or disclosure of information held by an agency or the loss of personal or non-personal information held by an agency where unauthorised access or disclosure is likely to occur.

|  |
| --- |
| **Personal information** is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity |

Section 47(1) of the IP Act provides that an **Eligible Data Breach** *always* involves personal information andinvolves an actual or potential loss of, unauthorised access to, or unauthorised disclosure of personal information, which is “likely to result in serious harm” to one person or more.

Section 47(2) of the IP Act prescribes factors to consider when assessing whether the likely harm is 'serious harm'. These factors include the kind of personal information disclosed, sensitivity of the personal information involved and the persons who have or may have obtained the personal information subject to the breach.

|  |
| --- |
| See OIC Guidance and the Template Response Plan for more information on the meaning of "*personal information*", "*unauthorised access*", "*disclosure*", "*loss of personal information*" and "*serious harm*". |

# **Examples of data breaches and Eligible Data Breaches**

**Not every data breach will be an Eligible Data Breach**.

A data breach can happen in various ways. Examples include: by malicious actions of third parties, internally due to human error, or a failure in information handling or security systems. However, not all data breaches will be an Eligible Data Breach and engage the MNDB.

An E**ligible Data Breach** under the IP Act involves personal information and may occur internally within an agency or involve the unauthorised access and/or disclosure of personal information by or to external parties, including threat actors or contractors.

Where a data breach involves personal information and any impacted individuals may be seriously harmed, then the data breach may be an **Eligible Data Breach**.

# **Key Principles in developing a Data Breach Policy**

The IP Act does not prescribe what must be included in a Data Breach Policy.

The variance in types and impacts of a data breach means there can be no "one size fits all" Data Breach Policy approach.

However, adopting best practice, there are six (6) Key Principles that agencies should consider and continue to consult as a touchstone in developing, operationalising and maintaining a Data Breach Policy:

|  |  |
| --- | --- |
| 1. | **Allow for flexibility**  Every agency is different, and every data breach incident is different. There is no one-size-fits-all solution and therefore, it is important that an agency's Data Breach Policy allows for sufficient flexibility in its application. |
| 2. | **Organisationally aware**  It is critical that the Data Breach Policy appropriately interacts with an agency's overall risk management strategy and relevant policies e.g. cyber security policy and fraud policy. |
| 3. | **Put the right people in the room**  The success of an agency's Data Breach Policy hinges on the involvement of every member of the organisation.Security and risk management professionals, legal counsel, information technology services, human resources, and communications should be involved in developing an agency's Data Breach Policy. |
| 4. | **Realistic**  An agency's strategy for managing a data breach, as outlined in the agency's Data Breach Policy and any Data Breach Response Plan, must be practical and achievable. |
| 5. | **Easy to read**  An agency's Data Breach Policy and any Data Breach Response Plan must be easy to read because everyone in an agency must understand and comply with them. |
| 6. | **Reflect multidisciplinary approach**  While ownership of an agency's Data Breach Policy and any Data Breach Response Plan will sit with a particular officer, its application must reflect a multidisciplinary approach across the agency. This is particularly important for privacy, legal and information security/cyber teams. |

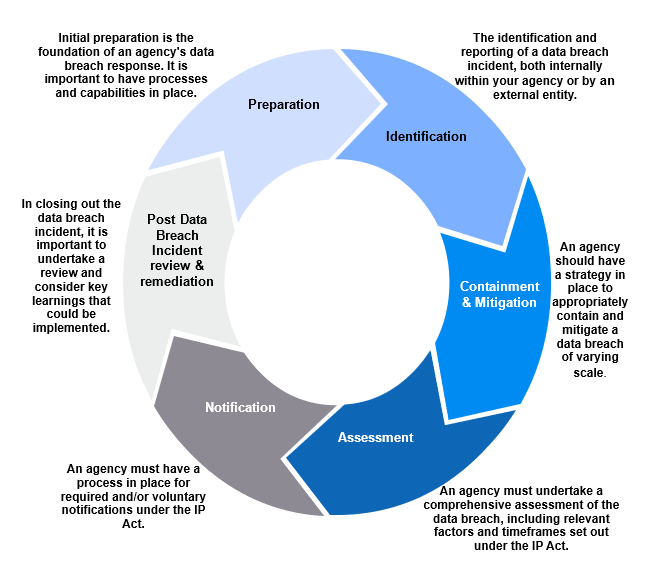
# **What to include in a Data Breach Policy**

Each data breach is different and will require a different response.

A Data Breach Policy should therefore set out (in a flexible way) how an agency will respond to a data breach, including 'Suspected Eligible Data Breaches'.

While a Data Breach Policy should not 'lock an agency into' a particular response to every data breach, the steps and actions to respond to a data breach can be split into six (6) distinct stages.

Guidance on each of these stages is provided below.



**Preparation is a critical first component of a Data Breach Policy and is necessary to establish the strong foundation necessary for robust responses to data breaches.**

A Data Breach Policy should identify what steps and actions have been taken by the agency to respond to a data breach. This can be an outline of the processes and procedures that an agency has put in place in order to respond to data breaches, noting that there will be variance across agencies in terms of the nature and scope of the steps and actions developed and implemented that will be undertaken by agencies.

However, as far as possible, a Data Breach Policy should outline the following areas in terms of preparatory steps and actions taken by an agency:

* the agency's key controls, systems and processes for identifying data breaches. This can include information about the key documents and procedures to be used in a data breach response, such as a Data Breach Response Plan, cyber incident response plan or information security policy
* how the Data Breach Policy interacts with the agency’s broader systems, policies, and procedures. As far as possible, these systems, policies and procedures should be specifically referenced – for example, cyber response, general incident or emergency management processes, communications strategies
* the agency’s strategy for ensuring it has the required capability and resourcing to respond to a data breach (for example, this may involve noting that the agency may engage outsourced cyber incident response service providers to manage complex incidents)
* clearly defined roles and responsibilities of agency officers and any internal bodies in responding to data breaches, noting that some agencies may have more detailed systems and processes, including internal mechanisms or bodies such as a Data Breach Response Team:
  + if an agency has an internal body of this nature, the Data Breach Policy should include information about this body, most notably, the roles and responsibilities of the members. Examples include decision-making roles for assessment and notification decisions, responsibility for overseeing reporting obligations, maintaining, testing, and updating the Data Breach Policy, recordkeeping, and post-breach review
  + depending on the agency's capabilities, an internal body's membership may include representatives from (at least) the agency's privacy, IT, cybersecurity, communications, HR and Legal branches, with Senior Executive involvement for serious a data breach. Subject matter expert teams may also need to be stood up depending on the source and nature of the data breach.
* an agency's approach to staff training activities and awareness in identifying, responding to, and managing a data breach, and
* an agency's testing and review mechanisms that enable it to prepare for (and identify key learnings from) a data breach.

|  |
| --- |
| **Drafting tip:**  Never include sensitive security information, for example, about controls and/or detection mechanisms, in a Data Breach Policy. Take care when describing an agency's controls and processes for identifying a data breach to ensure this description does not provide information which could be valuable to external threat actors or in any way undermine an agency's ability to identify and respond to a data breach. |

**The Identification component focuses on developing processes for detecting and identifying data breaches, including internal communication processes for considering and escalating (where necessary) a data breach. These measures are essential in enabling an agency to effectively contain a data breach and mitigate potential harms.**

Reflecting the critical nature of assessment and detection activities, a Data Breach Policy should as far as possible, outline and/or explain:

* what an actual or suspected data breach is, how one may occur, and the distinction between a data breach and an Eligible Data Breach and a Suspected Eligible Data Breach
* how the agency identifies a data breach, including through internal and external sources (for example, the public, another agency, or a Contracted Service Provider)
* how a data breach is reported and escalated internally (for example, by reporting a suspected incident to a Manager)
* the processes, systems and procedures that will be engaged to identify and assess a data breach, noting security concerns in referencing these processes, systems and procedures
* the circumstances in which a Data Breach Response Team or other similar internal body will be stood up (for a more serious data breach), the process to stand it up, and its composition:
  + to assist in identifying when a Data Breach Response Team or similar body will be stood up, use examples relevant to the agency's operating context
  + for example, an agency that handles a large volume of health information could provide scenarios touching on the actual ways that health information is collected, used, stored, and disclosed in practice, reflecting any known risk factors for that agency, and
  + these examples may also assist in helping staff identify how a breach might impact the agency, its functions, and the individuals whose information it handles.

|  |
| --- |
| **Drafting tip:**  Never assume a data breach only involves third party unauthorised access.  You should assume that human errors will be the most likely cause of a data breach and should design system and processes accordingly. This should include both technical controls to prevent poor practices (for example, implementing an automatic delay on an email being sent), and assurance testing to find and remediate issues (for example, penetration testing). |

**Containment and mitigation measures in a Data Breach Policy address, at a high level, the reasonable steps an agency will take to contain and mitigate a data breach.**

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

Noting these matters, a Data Breach Policy should outline the following:

* at a high level, the agency’s process for the initial evaluation of a suspected data breach in order to inform containment and mitigation strategies. This will include a risk assessment process, covering low, medium and high risk data breach scenarios
* whether the breach is, for example, lower risk (smaller scale / minor) or medium to higher risk (more significant / Suspected Eligible Data Breach). Each risk level requires a different approach, especially in the context of containment and mitigation and notification obligations. For example, the following considerations may inform what containment measures need to be taken:
  + what happened to cause the incident
  + can interim controls be implemented
  + how serious is the incident (i.e. what information and individuals are impacted)
  + does the agency need to work with any third parties to investigate and resolve the incident
  + is internal assistance from other business areas required (e.g. information security)
  + can the personal information be recovered
  + can the person who has received information incorrectly be contacted
  + can the system which has been breached be shut down
  + can the activity that led to the breach be stopped
  + can access codes or passwords be revoked or changed, and
  + did the data breach occur due to the actions of an external party (i.e. a cyber-attack).
* how the agency will contain and mitigate an actual or suspected data breach, including the containment and mitigation actions that mitigate any harms
* details of any specific roles and responsibilities including the Data Breach Response Team or similar body in containing and mitigating the risk in question, and
* where relevant, references to other policies and procedures that may be impacted by a data breach to ensure all necessary areas of the agency are involved and aware of the potential impacts of a data breach.

The following high-level guidance can inform an agency's risk assessment:

|  |  |
| --- | --- |
| **Nature and sensitivity of information** | **Sensitive information**  If the data breach involved sensitive information, the higher the risk of harm to the affected individuals.  **Publicity of the data**  In addition to sensitivity, the level of publicity already given to the information is also important. The agency should confirm whether the information was already (publicly) accessible.  **Linked personal data**  Data breaches involving health data, identity documents, or financial data, such as credit card information, are damaging in isolation, but combined with publicly available information, can pose additional risks of serious crimes such as identity theft. For that reason, linked personal information poses a greater risk than isolated personal information. |
| **Amount of information and number of affected individuals** | Consider the amount of information affected by the data breach and the total number of individuals whose personal information has been affected. The more data and individuals affected, the higher the risks. |
| **Ease of identifying the individuals** | Consider how easy it will be for a party with access to personal information to identify an individual (possibly after comparison with additional information available). The risk depends on whether individuals can be identified directly without any other personal information, or whether additional information from other categories of data is needed to identify the individuals. |
| **Seriousness of the harm** | The potential harm to the individuals, and the seriousness of the harm must be determined. Data breaches can be extremely damaging, cause physical harm, psychological stress, humiliation or reputational damage in cases such as identity fraud. If the data breach concerns the personal information of vulnerable individuals (e.g. patients, children), a higher risk of damage may be attributed. |
| **Existing mitigating measures** | Existing mitigating measures in place during the data breach should be considered in the overall risk assessment, by asking whether, and how, these measures protect the affected individuals. |

|  |
| --- |
| **Drafting tips:**  Take care when describing an agency's controls and processes for responding to a data breach to ensure this description does not provide information which could be valuable to external threat actors or in any way undermine an agency's ability to identify and respond to a data breach.  What if a breach involves more than one agency? The Data Breach Policy may address strategies for managing, responding to, and providing notice of a data breach involving other agencies – for example, documenting key contacts and defining roles and responsibilities for assessment, remediation, information flow, and notification to individuals and the Information Commissioner. |

**When a data breach occurs, an agency will need to comprehensively assess the risks associated with the breach. As the IP Act imposes specific obligations for an Eligible Data Breach, a Data Breach Policy needs to detail an agency’s assessment process for any data breach but also the process for specifically determining whether the data breach is an Eligible Data Breach for the purposes of the IP Act and the MNDB scheme.**

The assessment stage focuses on an assessment being conducted under section 48(2)(b) of the IP Act. Agencies must assess whether there is an Eligible Data Breach within 30 days of forming a reasonable suspicion of a data breach. However, if the agency is satisfied that it will be unable to complete the assessment in 30 days, it can extend that time under section 49 of the IP Act.

Section 48(2)(b) of the IP Act deals with the prospect that when a data breach is first identified, agencies may not have sufficient information to reach a level of certainty that the data breach is an Eligible Data Breach. Where this occurs and an agency only has a **reasonable suspicion** of an Eligible Data Breach, there is a requirement to rapidly **assess** whether there are **reasonable grounds** to believe the data breach is an Eligible Data Breach of the agency.

A Data Breach Policy should therefore look to outline the following:

* how the agency will make this assessment in accordance with the requirements of the IP Act, including assessing the breach's severity and the likelihood that it will result in serious harm to an individual
* the steps to take in assessing whether the data breach is an Eligible Data Breach as required under the MNDB scheme, including a list of factors indicating the likelihood of serious harm which should be considered as part of this assessment process
* how an agency will record and document the assessment
* where possible, a risk assessment process for the assessment of serious harm (or at least identify that a risk assessment should be undertaken as part of the assessment process and refer to other procedures such as the Data Breach Response Plan which may include an actual risk assessment process), and
* details of any specific roles and responsibilities including the Data Breach Response Team in the assessment process.

|  |
| --- |
| The relevant factors prescribed under the IP Act for assessing whether a data breach may result in serious harm to an individual are:   1. the kind of personal information accessed, disclosed or lost 2. the sensitivity of the personal information 3. whether the personal information is protected by 1 or more security measures 4. if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome 5. the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information 6. the nature of the harm likely to result from the data breach, and 7. any other relevant matter.   'Other relevant matters' will depend on the nature of the data breach, but the following considerations may also assist in assessing the seriousness of the data breach:   * what is the nature of the breach * is it likely that a counterparty or third party caused the breach * what is the seriousness of the breach * has the breach affected another agency * are there any vulnerabilities of the affected individuals e.g. involving children or a domestic violence victim-survivor * the effectiveness of the steps taken to control the breach e.g. has containment and mitigation lessened the risk * has there been unauthorised access, disclosure or loss of personal information that was collected by the agency, and * if so, would a reasonable person conclude the breach is likely to result in serious harm to an individual to whom the information relates. |

|  |
| --- |
| **Drafting tip:**  As the assessment process for an Eligible Data Breach is prescribed in the IP Act, a Data Breach Policy must accurately describe those requirements.  An agency's Data Breach Policy may contemplate the involvement of external experts to assist with managing a more complex data breach. |

**A Data Breach Policy should include a clear notification strategy that is consistent with sections 51 to 54 of the IP Act and enables quick and effective communication with the Information Commissioner, affected individuals and other external parties as required.**

The Data Breach Policy should set out the agency's obligations under the IP Act in relation to notification requirements under the MNDB scheme. These requirements include determining whether the data breach is subject to an exemption from the notification process as well as requirements regarding the information that must be provided to the Information Commissioner and/or the affected individual/s.

A Data Breach Policy should provide details in relation to how an agency deals with these requirements in undertaking the notification process.

|  |  |
| --- | --- |
| **Notification to the Information Commissioner** | Unless an exemption applies, agencies must notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an Eligible Data Breach.  Agencies may seek advice from the OIC about a data breach, but notification of an Eligible Data Breach must be made in writing.  Under section 51 of the IP Act, the agency must prepare and give the Information Commissioner a statement. |
| **Notification to individuals to whom the information the subject of the Eligible Data Breach relates** | Unless an exemption applies, as soon as practicable after forming a reasonable belief that a data breach is an Eligible Data Breach, an agency must take the steps set out in section 53 of the IP Act to notify particular individuals and provide them with the information required in section 53(2) of the IP Act. |

This component of a Data Breach Policy should therefore include an outline of the agency's notification strategy:

* the notification requirements under the MNDB scheme, including the exemptions that may apply to excuse notification, and who is responsible for formal notification
* a notification strategy that is clear and consistent with the statutory requirements of the MNDB scheme. The strategy should identify how individuals will be notified, and who will take responsibility for notification decisions.
* a strategy for voluntary notification – even if notification is not mandatory under the IP Act, there should be a process for making voluntary notifications. For example, this may be appropriate in circumstances where the public would be unlikely to accept a technical argument as to why the agency was not responsible for a data breach as opposed to a third party contractor
* how to determine when individuals must be notified
* key contacts for communications
* how individuals will be contacted and notified in accordance with section 53 of the IP Act, and how communications with affected individuals will be managed, including how any inquiries will be made of disclosing agencies under section 54 of the IP Act
* details of the process required to be undertaken to record the Eligible Data Breach in the Eligible Data Breach Register
* a broader communications strategy, including for example responsibility for consulting with any external stakeholders, contractors or other third parties who may be impacted by the data breach, and
* as the notification process for an Eligible Data Breach is prescribed in the IP Act, the Data Breach Policy must be clear about what is required under the IP Act.

|  |
| --- |
| **Notification tips** |
| **When to notify particular individuals**  Individuals/ organisations affected by a data breach will be notified as soon as practicable. However, the agency will need to ensure they have sufficient information about the breach before issuing notifications. Premature notifications are not recommended and may cause unnecessary harm, panic, and concern. |
| **How to notify particular individuals**   1. How affected individuals/organisations affected by the data breach are notified will depend on the type and scale of the breach, as well as the immediate practical issues such as having contact details for the affected individuals/ organisations. 2. Option 1: Notify each individual 3. If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, the agency must take reasonable steps to notify each individual of the required information directly. This may include by telephone, letter, email or in person.   Option 2: Notify each affected individual   * If Option 1 does not apply, agencies must take reasonable steps to notify each affected individual of the required information for the data breach, if doing so is reasonably practicable. * Under sections 47(1)(a)(ii) and (b)(ii) of the IP Act, an ‘affected individual’ is someone to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.   Option 3: Publish Information  If the agency cannot directly notify each individual (Option 1) or each affected individual (Option 2), it must publish the required information on its website for a period of at least 12 months, in accordance with section 53(1)(c) of the IP Act. An agency is not required to include information in its notice if it would prejudice its functions. An agency must advise the Information Commissioner how to access the notice and the Commissioner is required to publish the notice on the Commissioner's website for at least 12 months. |
| **What to include in notification to particular individuals**  Section 53(2) of the IP Act sets out the specific information that a notification must include, to the extent it is reasonably practicable:   * + 1. the date that the breach occurred     2. a description of the breach     3. how the breach occurred     4. the personal information included in the breach     5. the amount of time the personal information was disclosed for     6. actions that have been taken or are planned to secure the information, or to control and mitigate the harm     7. recommendations about the steps an individual should take in response to the breach     8. information about complaints and reviews of agency conduct     9. the name of the agencies that were subject to the breach, and     10. contact details for the agency subject to the breach or the nominated person to contact about the breach. |

**After a data breach has been dealt with, 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.**

A Data Breach Policy should include the following information:

* who is responsible for the post-breach review and remediation process (determined by the nature and scale of the data breach. For example, where a Data Breach Response Team has been activated, this Team would likely conduct the review and remediation process). Consider also allocating responsibility for actioning the learnings from this process, as well as oversight and monitoring of the process
* a high-level overview of the process adopted to conduct the post-breach review and remediation, analysing all aspects of the data breach to identify key learnings, including details of remediation activities
  + what is required to remediate will be determined by the nature and scale of the data breach. This is particularly relevant to building an agency's corporate knowledge around data breach responses, and will assist in mitigating future risks of reoccurrence or similar breaches, and improving personal information handling processes in line with community and regulator expectations
* the process for conducting a post-response assessment of the response to the breach and the effectiveness of the Data Breach Policy. As an example, a review of any key learnings from the data breach and potential changes that should be made to prevent or reduce a risk of reoccurrence, and a prompt to consider revising and updating systems, processes and procedures relevant to data breaches
* a process for ensuring an accurate record of the data breach is captured, maintained and reported as appropriate (and who is responsible for this), and
* that any Eligible Data Breach will be recorded in the agency's Register of Eligible Data Breaches.

|  |
| --- |
| **Drafting tip:**  There should be a single repository of information documenting a data breach and response, as well as documents recording the decision-making process, including minutes of meetings, discussions and other key decision-making points.  This will be consistent with the agency's recordkeeping obligations under the *Public Records Act 2023* (Qld). |

# **Data Breach Policy Template**

ATemplate is provided to support agencies in preparing a Data Breach Policy in accordance with the IP Act.

This Template should 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 Guideline on OIC’s website, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au** |

Data Breach Policy Template

1. Purpose and Scope

*This section may provide:*

* *an explanation that an agency must have a Data Breach Policy under the IP Act outlining the steps it will take to respond to a data breach, including a Suspected Eligible Data Breach*
* *an overview of why a Data Breach Policy is important, why the agency has the data breach policy and a high level overview of what is included in the Data Breach Policy*
* *how the Data Breach Policy fits with the agency's internal and external documents, including privacy and cyber policies, and*
* *to whom the Data Breach Policy applies (e.g. all employees, including volunteers and contractors, in relation to all their work work-related dealings with each other and with customers, contacts or clients).*

1. Definitions

*This section can explain any defined terms used in the Data Breach Policy. Example definitions are provided at Appendix A.*

1. Roles and Responsibilities

*An example list of "Roles and Responsibilities" is provided below:*

| *Role* | *Responsibility* |
| --- | --- |
| *Employee* | *Read the Data Breach Policy and 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.*  *Where required in accordance with this Data Breach Policy, immediately report a data breach or suspected data breach to the appropriate officer (this could be a supervisor, manager, senior officer or privacy officer).*  *Respond to requests for information from and cooperate with the Privacy Officer and/or the Data Breach Response Team.*  *Comply with record keeping obligations.* |
| *Privacy Officer [or the relevant officer with privacy responsibilities]* | *Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates.*  *Escalate serious data breaches to relevant senior officer or executive.*  *Notify (or arrange for a senior officer or executive to notify) the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to the agency website under section 53(1)(c).*  *Immediately report a data breach that is also a cyber security incident to the Chief Information Officer, if not already reported.*  *Maintain the Register of Eligible Data Breaches.* |
| *Manager* | *Identify and escalate concerns within area of responsibility which may enliven the requirements of this Data Breach Policy.*  *Immediately report a data breach that is also a cyber security incident to the Chief Information Officer, if not already reported.* |
| *Senior Management*  *[for example: Chief Information Officer or executive]* | *Immediately report a cyber security incident that is also a data breach to the Privacy Officer, if not already reported.*  *Where relevant, notify the Information Commissioner, affected persons and others where required.*  *Implement the Cybersecurity Management Plan and related procedures if the data breach is also a cyber security incident.*  *Convene the Data Breach Response Team, when appropriate* |
| *Data Breach Response Team [note that members may be co-opted from various teams within the agency]* | *Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems.* |
| *Responsible Officer* | *Maintain and update this Policy.* |

1. Responding to a Data Breach
   1. Stage 1: Preparation
   2. Stage 2: Identification
   3. Stage 3: Containment and Mitigation
   4. Stage 4: Assessment
   5. Stage 5: Notification
   6. Stage 6: Post-data-breach review and remediation
2. Register of Eligible Data Breaches

*Under section 72 of the IP Act, agencies must keep an internal Register of Eligible Data Breaches. This section may note the need to keep the Register of Eligible Data Breaches up to date.*

*The OIC has developed an Eligible Data Breach Register Template.*

1. Record keeping

*This section may explain an agency's processes for documenting the management and response to an actual or suspected data breach, including an Eligible Data Breach.*

1. Related Legislation and Policies

*This section may list related laws, policies, procedures and other instruments. For example, the Data Breach Policy might be developed alongside a Data Breach Response Plan, which could be an internal document detailing the agency's more specific processes in managing and responding to a data breach.*

*The OIC has developed a Data Breach Response Plan Template.*

Appendix A Definitions

| Term | Meaning |
| --- | --- |
| 1. Agency Worker | A person who carries out work in any capacity for an agency as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including work as:   * 1. an employee   2. a contractor or subcontractor or an employee of a contractor or subcontractor   3. an apprentice or trainee   4. a student gaining work experience, or   5. a volunteer. |
| 1. Affected individual | An “affected individual” under section 47(1)(ii) of the IP Act. |
| 1. Australian Information Commissioner | The Australian Information Commissioner. |
| 1. Commonwealth Privacy Act | The *Privacy Act 1988* (Cth). |
| 1. Data breach | The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act. |
| 1. Data Breach Policy | This Policy. |
| 1. Data Breach Response Plan | A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing the agency's more specific processes in managing and responding to a data breach. |
| 1. Eligible Data Breach | An “Eligible Data Breach” will have occurred under section 47 of the IP Act where:   * 1. 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**   * 1. 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. |
| 1. Information Commissioner | The Queensland Information Commissioner. |
| 1. IP Act | The *Information Privacy Act 2009* (Qld). |
| 1. *Held* or *hold* in relation to personal information | Personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency. |
| 1. Personal information | Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:   * 1. whether the information or opinion is true or not, and   2. whether the information or opinion is recorded in a material form or not. |
| 1. Serious harm | To an individual in relation to the unauthorised access or unauthorised disclosure of the individual’s personal information, includes, for example:   * 1. serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or   2. serious harm to the individual’s reputation because of the access or disclosure. |
| 1. TFN | A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes. |