Data Breach Policy

Purpose and Scope

From 1 July 2025 Section 73 of the *Information Privacy Act 2009* (Qld) (**IP Act**) requires the Valuers Registration Board of Queensland (the Board) to prepare, and publish on its website, a Data Breach Policy detailing how the Board will respond to a data breach including data breaches that are Eligible Data Breaches or a Suspected Eligible Data Breach.

The Mandatory Notification of Data Breach (**MNDB**) scheme requires the **Board** 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.

This **Data Breach Policy o**utlines the Board's overarching policy in responding to data breaches, including 'Suspected Eligible Data Breaches'. It provides a high-level description of the 6 stages the Board will follow when responding to a Data Breach.

A separate **Data Breach Response Plan** has also been developed that contains much of the same information contained within this Policy for responding to an actual data breach, including 'Suspected Eligible Data Breaches', in accordance with the IP Act and best practice.

A hard copy of this Policy and its attachments is to be maintained by the VRBQ Secretary in the event that the VRBQ ICT systems are unavailable when access to this Policy and the Data Breach Response Plan is required.

Definitions

Definitions are provided at Appendix A of this document.

Roles and Responsibilities

Role	*Responsibility*
Administrative Assistant/Investigators	*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 (in most instances, this would be the Board Secretary, however, it could also include a Board Member)* *Respond to requests for information from and cooperate with the Secretary and/or the Data Breach Response Team.* *Comply with record keeping obligations.*

Role	Responsibility
Secretary	*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.* *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.* *Advise Board Members and Department representative of the data breach and plans to address the matter.* *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* *Maintain and update this Policy.*
Department Representative	*Provide a communication channel between the Board, the Department, and the Minister's Office to advise of any data breach as they occur.*
Board Member *Board Chair*	*Immediately report a cyber security incident that is also a data breach to the Secretary, 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 (due to the Board's small size this will usually consist of the Secretary and a Board Member, and will largely rely on external parties to assist)	*Manage a data breach that is considered likely to cause serious harm to any impacted individual or the agency's systems. The Secretary will lead the response and, where appropriate, seek assistance from the Board's Website Provider, IT Support Provider, the Queensland Government Cyber Security Unit, and any other party that is considered appropriate. Appendix C contains contact details for Board's main IT Suppliers/Support.*

Responding to a Data Breach

Stage 1: Preparation

The information contiained in this **Data Breach Policy** also provides a high-level overview of the 6 stages involved in how the Board will respond to a **data breach**, including a “Suspected Eligible Data Breach”, including Preparation, Identification, Containment and Mitigation, Assessment, Notification, and Post-Data-Breach Review and Remediation. The separate **Data Breach Response Plan** provides a more detailed 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.

The Board recognises that every data breach incident is different and there is no one size fits all solution. As a result, the Board supports flexibility within this policy and the associated **Data Breach Response Plan** to ensure that the aims of the legislation are met. The Board also recognises that a team approach is often required to address data breach issues and will appoint members to the Data Breach Policy Team as appropriate.

The Board will continue to undertake its usual annual IT Architecture review to ensure it understands the software platforms it has in place and the data contained within each, the underlying security protocols that support these platforms and the data they contain, and has the contact details for third party providers should assistance with a data breach be required.

The Board may rely on assistance from the Queensland Government Cyber Security Unit, the Department of Natural Resources and Mines, Manufacturing and Regional and Rural Development, and/or 3rd party suppliers to assist in responding to a data breach.

When an incident arises, the Board will establish a **Data Breach Response Team** consisting of the Board Secretary and a Board Member (appointed by the Board Chair) to take responsibility for implementing the **Data Breach Policy** and the **Data Breach Response Plan**.

The Board’s **Data Breach Response Plan** provides a step-by-step guide on the Board’s response process and the resources it can activate to respond to a data breach.

The Secretary is responsible for ensuring that any decisions and outcomes made during the **Data Breach Response Plan** process are appropriately documented and retained for each complaint matter.

Stage 2: Identification

The Identification process focuses on the processes to detect and identify data breaches, and the communication processes to consider and escalate (where necessary) a data breach.

A **data breach** is defined in the IP Act to mean the unauthorised access or disclosure of information held by the Board or the loss of personal or non-personal information held by the Board 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

An "Eligible Data Breach" will have occurred under section 47 of the IP Act where:

(a) 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**

(b) 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.

All data breaches, or suspected data breaches, should be reported to the Secretary, who will then discuss with the Board Chair about forming a **Data Breach Response Team** to determine if an **Eligible Data Breach** has occurred and what, if any, response is required.

An example of an internal reporting mechanism includes a staff member suspects there has been a data breach, they will immediately contact the Secretary and provide all relevant information. The Secretary will then conduct an immediate risk assessment of the breach and contact the Board Chair to determine if to escalate the matter and establish a Data Breach Response Team. The Data Breach Response Team will use this Policy and the Data Breach Response Plan to establish a proactive and reactive communication strategy and consider the appropriateness of any immediate notifications. The Data Breach Response Team will also consider engaging external parties to assist with managing the data breach (for example, representatives at the Department, legal counsel, the Queensland Government Cyber Security Unit, technical support, media and communications experts, etc.).

Some examples of an **Eligible Data Breach** might include the Secretary emailing personal complaint information to an incorrect email address in error, or a Board or Staff Member accidently losing or misplacing documents containing sensitive or personal information.

Some examples of less serious data breaches might include sending a generic email to the wrong recipient (only a few unintended recipients) or accidentally disclosing contact details to a trusted contractor or another government agency.

The Board relies on advice from 3rd party suppliers if data has been breached on any SaaS platforms.

The Secretary is responsible for ensuring that decisions made regarding the Identification process are appropriately documented and retained for each data breach matter.

Stage 3: Containment and Mitigation

The **Data Breach Response Team** will undertake an initial evaluation of the suspected data breach in order to determine what containment and mitigation strategies should be applied.

The **Data Breach Response Plan** outlines the processes involved for the **Data Breach Response Team** to undertake a risk assessment. This will consider factors such as the sensistivity of the data, the seriousness of the harm, if the information was already publicly available, and the number of individuals addected.

The **Data Breach Response Team** will also consider what conainment measures may need to be taken. As part of this process it will consider issues such as what happened to cause the incident, can interim controls be implementedhow serious is the incident, who does the Board need towork with to investigate and resolve the matter, did the data breach occur duie to the actions of internal or external parties, can access codes or passwords be changed, etc.

Using the information gealeaned form the above process, the Data Breach Response Team will develop a response to contain and mitigate the actual or suspected data breach, including the containment and mitigation actions that mitigate any harms.

The Secretary is responsible for ensuring that the decisions made regarding Containment and Mitigation are appropriately documented and retained for each complaint matter.

Stage 4: Assessment

When a data breach occurs, the Board will need to comprehensively assess the risks associated with the breach. As the IP Act imposes specific obligations for an Eligible Data Breach, this Data Breach Policy needs to detail the Boards 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.

An “Eligible Data Breach” will have occurred under section 47 of the IP Act where:

(a) 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**

(b) 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.

The assessment stage focuses on an assessment being conducted under section 48(2)(b) of the IP Act. The Board must assess whether there is an Eligible Data Breach within 30 days of forming a reasonable suspicion of a data breach. However, if the Board 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, the Board may not have sufficient information to reach a level of certainty that the data breach is an Eligible Data Breach. Where this occurs and the Board 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 Board.

In making an assessment, the Board should consider the guidance provided in the previous section regarding risk assessment. The Board also needs to assess if a data breach will cause serious harm.

The relevant factors prescribed under the IP Act for assessing whether a data breach may result in serious harm to an individual are:

a) the kind of personal information accessed, disclosed or lost
b) the sensitivity of the personal information
c) whether the personal information is protected by 1 or more security measures
d) if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome
e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
f) the nature of the harm likely to result from the data breach, and
g) 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.

In addition to undertaking its own assessment, the Board may also wish to access the Data Breach Assessment Tool. This tool provides the Board with a structure to conduct the assessment with associated advice for consideration at each step of the process. The tool can also be used to support the initial consideration of a data breach to help inform an agency's next steps.

The result or recommendation provided by the tool is only a guide, and nothing in this tool comprises legal advice.

Each breach requires consideration of its specific circumstances, and while this tool assists agencies, a comprehensive and objective assessment is required before decisions are made. The tool can be accessed at: https://oic.advancedforms.squiz.cloud/form/mandatory-notification-data-breach-mndb-scheme

It is a requirement that the deliberations and outcomes of the Data Breach Response Team assessment process are documented and retained for each data breach matter. It is the responsibility of the Secretary to ensure this occurs.

Stage 5: Notification

Section 51 to 54 of the IP Act outlines the notification requirements that the Board must meet to satisfy its legislative obligations. This section outlines the notification requirements, provides some information that should information the Data Breach Response Team on how it should respond, and then provides space for the Data Breach Response Team to record the actions that it will take in regard to this matter.

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.

Notification tips

When to notify particular individuals
Individuals/organisations affected by a data breach will be notified as soon as practicable after the Board has 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
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. Some options include: -

Option 1: Notify each individual
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:

(a) the date that the breach occurred
(b) a description of the breach
(c) how the breach occurred
(d) the personal information included in the breach
(e) the amount of time the personal information was disclosed for
(f) actions that have been taken or are planned to secure the information, or to control and mitigate the harm
(g) recommendations about the steps an individual should take in response to the breach
(h) information about complaints and reviews of agency conduct
(i) the name of the agencies that were subject to the breach, and
(j) contact details for the agency subject to the breach or the nominated person to contact about the breach.

The Secretary is responsible for ensuring that the decisions made regarding notification are appropriately documented and retained for each complaint matter.

Stage 6: Post-data-breach review and remediation

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.

It is the responsibility of the Date Breach response team to provide this report to the full Board for their review and consideration. On sign-off from the Board, it is then the responsibility of the Secretary to ensure that documentation regarding the Data Breach and the actions taken by the Board are appropriately recorded and retained. This should include documents recording the decision-making process, minutes of meetings, discussions, and other key decision-making points.

The Board's Register of Eligible Data Breaches is to be updated to reflect that the matter has been completed.

Register of Eligible Data Breaches

The Board is required to keep and maintain a Register of Eligible Data Breaches as per section 72 of the IP Act. It is the Secretary's responsibility to maintain this register and keep it up to date.

Record keeping

It is the responsibility of the Secretary to document and retain the Board's management and response to an actual or suspected data breach, including an Eligible Data Breach.

Related Legislation and Policies

Information Privacy Act 2009 (Qld)
Privacy Act 1988 (Cth)
Valuers Registration Act 1992
Valuers Registration Regulations 2024
Valuers Registration Amendment Regulations 2025

Appendix A Definitions

Term	Meaning
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: an employee a contractor or subcontractor or an employee of a contractor or subcontractor an apprentice or trainee a student gaining work experience, or a volunteer.
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act.
Australian Information Commissioner	The Australian Information Commissioner.
Commonwealth Privacy Act	The *Privacy Act 1988* (Cth).
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.
Data Breach Policy	This Policy.
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.
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of 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.
Information Commissioner	The Queensland Information Commissioner.
IP Act	The *Information Privacy Act 2009* (Qld).
***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.

Term	Meaning
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	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.
TFN	A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.