Queensland Independent Renumeration Tribunal

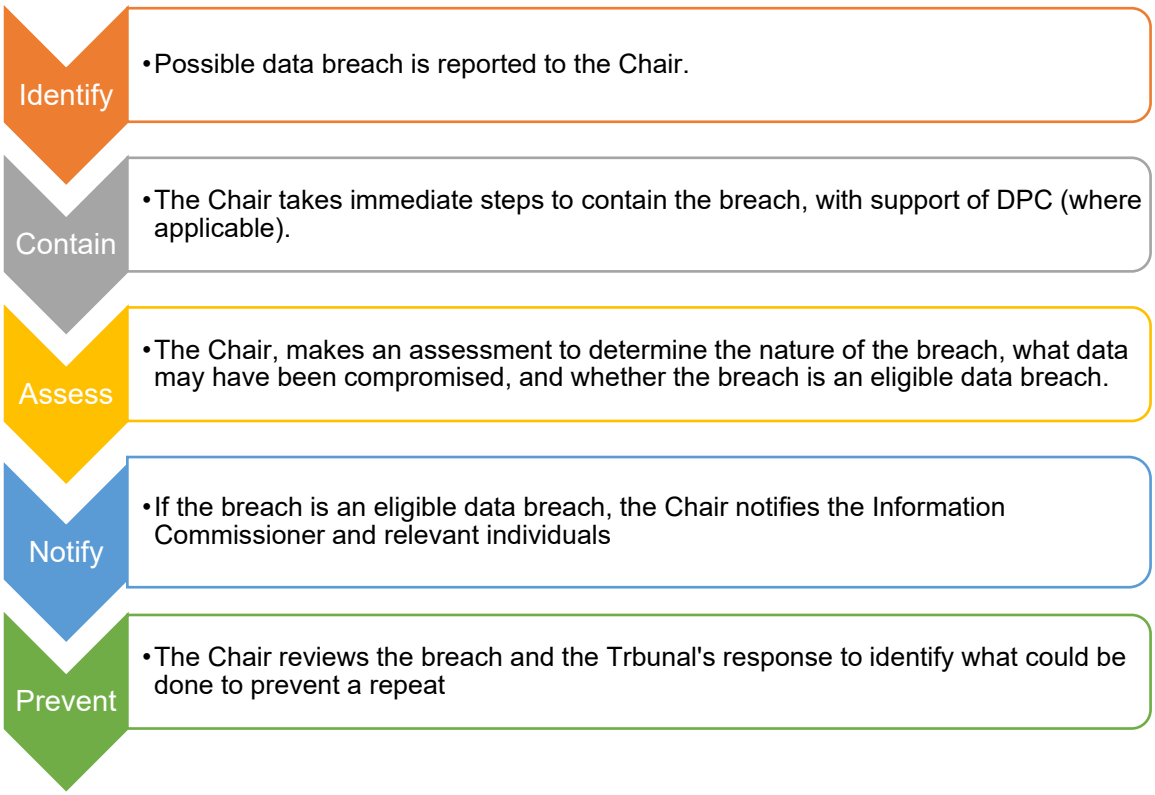
Data Breach Policy

1. Purpose and Scope

This Data Breach Policy (the Policy) outlines the steps the Queensland Independent Remuneration Tribunal (QIRT) will take to respond to a data breach including a Suspected Eligible Data Breach to meet obligations under the *Information Privacy Act 2009* (IP Act).

2. Responding to a data breach

Some data is stored with the Department of the Premier and Cabinet, via the secretariat function. Our response to a potential data breach generally follows the steps below:



Step 1: Identifying a data breach

It is the responsibility of all Tribunal members to report a data breach or possible data breach to the Chair of the Tribunal (the Chair) immediately. If unsure whether a breach has occurred, they should err on the side of caution and report the incident to the Chair. The Chair should always be the first point of contact if a data breach is suspected.

Step 2: Containing a data breach

Once informed of a suspected data breach, the Chair will take steps to immediately contain the breach and as soon as practicable take remedial action to prevent or lessen the likelihood the breach will result in harm to any individual.

Step 3: Assessing a data breach

The Chair must assess whether the data breach is an eligible data breach (See Definitions in section 4)**.**

To determine whether the breach is an eligible data breach, the Chair must ascertain whether the information in question is personal information as defined in the IP Act **and** whether an individual affected by the breach is likely to experience serious harm (See Definitions in section 4). Both limbs must be met for the breach to qualify as 'eligible.' Regarding the second limb, harm must be both serious **and** likely.

Under the IP Act, the assessment must be completed within 30 days, unless the Chair extends the assessment period and gives written notice to the Information Commissioner of the extension.

Step 4: Notification of a data breach

If the data breach is determined to be an eligible data breach, the Chair will take steps to notify the Information Commissioner, relevant individuals and other agencies of the breach in accordance with the notification requirements in the IP Act, unless relevant exemptions under the IP Act apply.

In some circumstances, it may be appropriate or necessary to notify other third parties of the breach. This could include the following:

- Queensland Police Service if the breach appears to involve theft or other criminal activity
- Crime and Corruption Commission if the breach involves corrupt conduct within the meaning of the *Crime and Corruption Act 2001*.

Any further notifications will only be made with the approval of the Chair.

Step 5: Eligible Data Breach Register

The Chair will ensure that appropriate records of the data breach are maintained in the Tribunal's Eligible Data Breach Register in accordance with the IP Act.

Step 6: Post breach review

After a data breach, the circumstances of the breach will be considered by the Chair for any actions required to prevent a similar breach in the future.

3. Legislation

Information Privacy Act 2009

4. Definitions

Term	***Definition***
Data Breach	Data breach of an agency means either of the following: a) an unauthorised access to, or unauthorised disclosure of, information; or b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur. Refer Schedule 5 Dictionary *Information Privacy Act 2009*
Eligible data breach	An Eligible Data Breach occurs when: (i) there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; **and** (ii) (ii) the unauthorised access or disclosure of the information is likely to resulting serious harm to an individual. An 'eligible data breach' only involves personal information. Refer section 47 *Information Privacy Act 2009*
Eligible Data Breach Register	The IP Act requires agencies to keep a register of Eligible Data Breaches. The register must include prescribed information set out in section 72 of the IP Act.
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: a) whether the information or opinion is true or not; and b) whether the information or opinion is recorded in a material form or not. Refer section 12 *Information Privacy Act 2009*
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example – (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or (b) serious harm to the individual's reputation because of the access or disclosure. Refer Schedule 5 Dictionary *Information Privacy Act 2009*

POLICY ADMINISTRATION

1. Revision History

Revision date	Version Number	Author	Description of changes
June 2025	*1.0*	Gina McCabe	Initial draft

2. Approval

Position	Date
Queensland Independent Remuneration Tribunal	*3 July 2025*