

# Queensland Veterans Council

## Data Breach Policy

### 1. Purpose and Scope

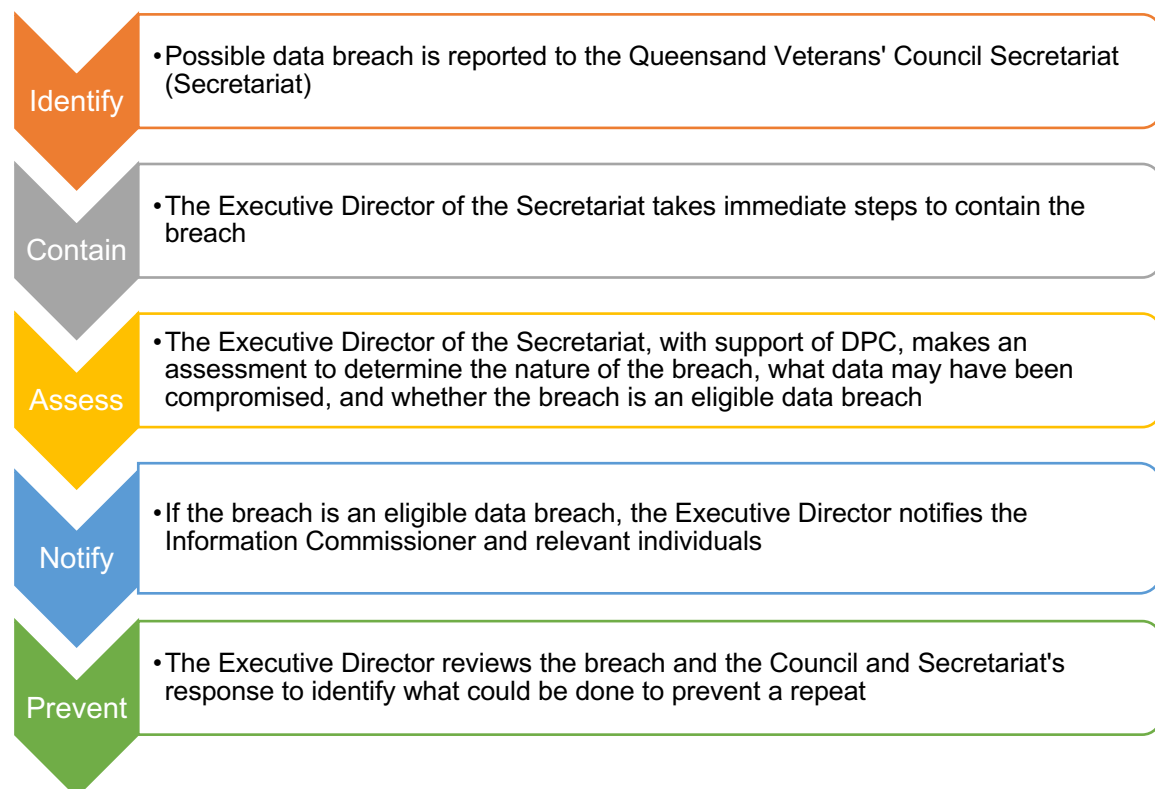
This Data Breach Policy (the Policy) outlines the steps the Queensland Veterans Council (the Council) will take to respond to a data breach including a Suspected Eligible Data Breach to meet its obligations under the *Information Privacy Act 2009* (IP Act).

The Department of Premier and Cabinet (DPC) provides administrative support to the Council as required under the *Queensland Veterans Council Act 2021* and therefore a number of administrative functions and operations for the QVC are undertaken by DPC in support of the QVC.

A cyber incident of information systems issue that affects Veterans Queensland is out of scope for this policy and will be managed under the DPC Data Breach Policy.

### 2. Responding to a data breach

Our response to a potential data breach generally follows the steps below:



#### Step 1: Identifying a data breach

It is the responsibility of all Council and Secretariat members to report a data breach or suspected data breach to the Executive Director immediately. If unsure whether a breach

has occurred, they should err on the side of caution and report the incident to the Executive Director. The Executive Director should always be the first point of contact if a data breach is suspected.

The Executive Director will immediately report a data breach or suspected data breach to the Privacy Contact Officer of DPC.

### ***Step 2: Containing a data breach***

Once informed of a suspected data breach, the Executive Director and DPC Privacy Contact Officer 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 Executive Director and DPC Privacy Contact Officer, with support of the Secretariat and the DPC privacy team, 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 Executive Director and DPC Privacy Officer 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 Executive Director 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 Executive Director 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 Executive Director.

### ***Step 5: Eligible Data Breach Register***

The Executive Director will ensure that appropriate records of the data breach are maintained in the Council'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 Executive Director, the DPC Privacy Officer and the Council for any actions required to prevent a similar breach in the future.

### 3. Legislation

*Information Privacy Act 2009*

### 4. Definitions

<b>Term</b>	<b>Definition</b>
<i>Data Breach</i>	<p>Data breach of an agency means either of the following:</p> <ul style="list-style-type: none"><li>a) an unauthorised access to, or unauthorised disclosure of, information; or</li><li>b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.</li></ul> <p>Refer Schedule 5 Dictionary <i>Information Privacy Act 2009</i></p>
<i>Eligible data breach</i>	<p>An Eligible Data Breach occurs when:</p> <ul style="list-style-type: none"><li>(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; <b>and</b></li><li>(ii) (ii) the unauthorised access or disclosure of the information is likely to resulting serious harm to an individual.</li></ul> <p>An 'eligible data breach' only involves personal information.</p> <p>Refer section 47 <i>Information Privacy Act 2009</i></p>
<i>Eligible Data Breach Register</i>	<p>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.</p>
<i>Personal Information</i>	<p>Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:</p> <ul style="list-style-type: none"><li>a) whether the information or opinion is true or not; and</li><li>b) whether the information or opinion is recorded in a material form or not.</li></ul> <p>Refer section 12 <i>Information Privacy Act 2009</i></p>
<i>Serious harm</i>	<p>To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example –</p> <ul style="list-style-type: none"><li>(a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or</li></ul>

<b><i>Term</i></b>	<b><i>Definition</i></b>
	<p>(b) serious harm to the individual's reputation because of the access or disclosure.</p> <p>Refer Schedule 5 Dictionary <i>Information Privacy Act 2009</i></p>