Premier and Minister for Veterans

Data Breach Policy

1. Purpose and Scope

This Data Breach Policy (the Policy) outlines the steps the Premier and Minister for Veterans and their Office (the Premier's Office) 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). This Policy also applies the Assistant Minister to the Premier on Matters of State and New Citizens and the Assistant Minister to the Premier for Cabinet and South West Queensland (the Assistant Ministers). References to the Premier's Office in this Policy includes the Assistant Ministers.

This Data Breach Policy outlines how the Premier's Office meets its obligations under the *Information Privacy Act 2009* (IP Act) to:

- prepare and publish a data breach policy
- contain a data breach and mitigate harm caused by the data breach
- comply with notification requirements for eligible data breaches
- maintain a register of eligible data breaches.

Collectively, these requirements are known as the Mandatory Notification of Data Breach (MNDB) Scheme.

A cyber incident or information systems issue that affects the Ministerial intranet or email server is out of scope for this policy and will be managed under the Department of the Premier and Cabinet (DPC) Data Breach Policy.

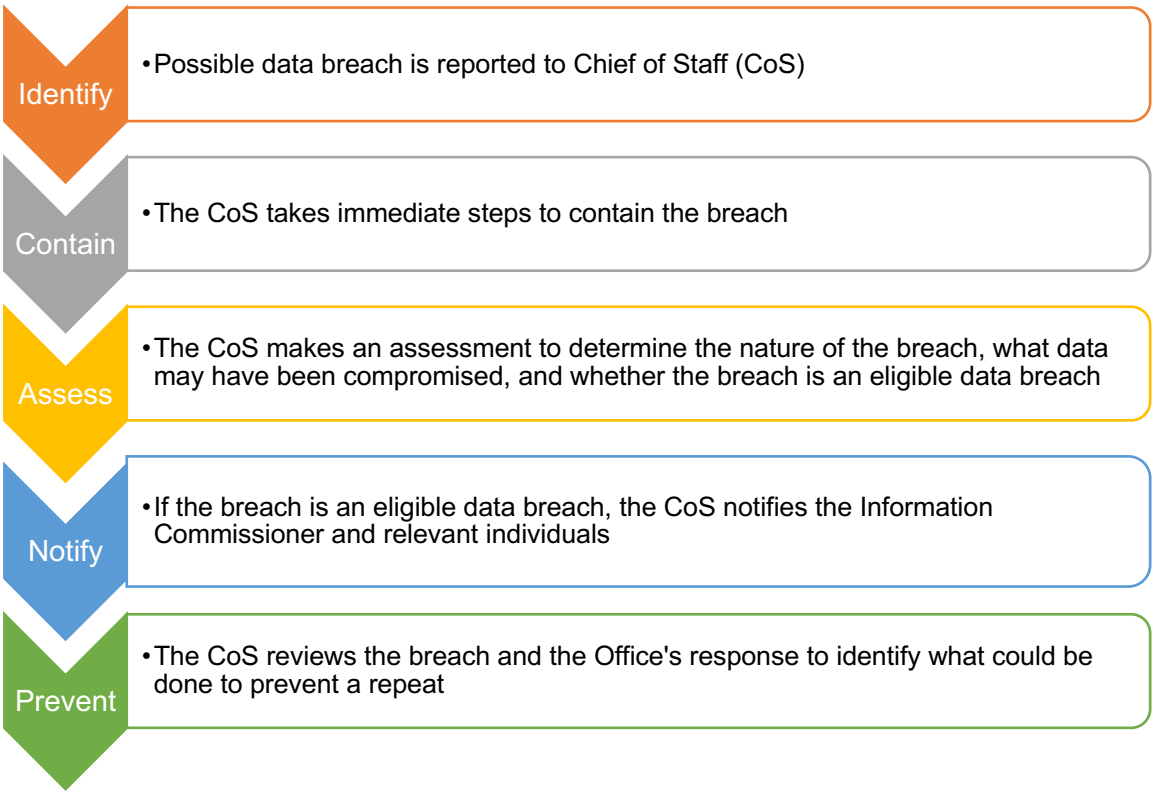
2. Proactive readiness for a potential data breach

The Office ensures readiness for a potential data breach through:

- *Privacy training and awareness* – employees will receive training on how to deal with potential data breaches as part of standard privacy training
- *Information security measure*s and *Incident management measures* provided by DPC.

3. 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 staff members to report a data breach or possible data breach to the CoS immediately. If the staff member is unsure whether a breach has occurred, they should err on the side of caution and report the incident to the CoS. The CoS should always be the first point of contact if a data breach is suspected.

Step 2: Containing a data breach

Once informed of a possible data breach, the CoS 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 CoS must assess whether the data breach is an eligible data breach **(**see Definitions in section 6**).**

To determine whether the breach is an eligible data breach, the CoS 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 6). 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 CoS 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 CoS 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 CoS.

Step 5: Data Breach Register

The CoS will ensure that appropriate records of the data breach are maintained in the Office's Mandatory 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 CoS for any actions required to prevent a similar breach in the future.

4. Legislation

Information Privacy Act 2009

5. Definitions

Term	***Definition***
CoS	Chief of Staff to the Premier and Minister for Veterans
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**

Term	***Definition***
	(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*
Ministerial staff member	A person employed under the *Ministerial and Other Office Holder Staff Act 2010*.
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

Approver	Date
Office of the Premier	30/06/2025