Department of the Premier and Cabinet Data Breach Policy

Last updated: June 2025

Data Breach Policy

1. Policy Statement

The Department of the Premier and Cabinet (DPC) has a duty to protect the data it holds from misuse and act swiftly and effectively in the event of a data breach. Swift identification, assessment, containment, and mitigation of harm of a data breach supports DPC's wider commitment to strong privacy arrangements, respect for individual privacy, and effective legislative compliance.

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

- prepare and publish a data breach policy
- contain an Eligible Data Breach, including a suspected Eligible Data Breach, and mitigate harm caused by the data breach
- comply with notification requirements for Eligible Data Breaches to Information Commissioner and particular individuals affected by the breach
- maintain a register of Eligible Data Breaches.

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

Implementation of this Data Breach Policy will also assist in mitigating DPC's Enterprise Risk categories relating to asset and information, trust and reputation, and governance and financial impact.

2. Scope

This policy sets out the steps DPC will take when responding to an Eligible Data Breach or suspected Eligible Data Breach under the MNDB scheme.

The policy applies to all DPC employees involved in handling or managing data.

3. Meaning of 'data breach' and 'Eligible Data Breach'

The IP Act contains two concepts: 'data breach' and 'Eligible Data Breach.' A data breach involves information held by the agency (not just personal information).

The IP Act defines a data breach as unauthorised access to, or unauthorised disclosure of, the information **or** the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

An Eligible Data Breach involves personal information and must involve **both** of the following:

- 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**

- the unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').

The reason the IP Act distinguishes between these two types of breaches is because only an Eligible Data Breach must, subject to prescribed exceptions, be notified to the Information Commissioner, relevant individuals and other agencies.

A data breach may involve human error, information misuse by an employee, a system fault or a malicious criminal attack.

- Examples of human error can include emailing or mailing information to the wrong recipient or losing agency-owned devices, such as a laptop or phone or agency hard-copy documents.
- Examples of information misuse by an employee can include unauthorised access to information the employee is not entitled to view and inappropriate use or disclosure of information in contravention of internal policies and Queensland Privacy Principle (QPP) obligations.
- Examples of system faults may include the disclosure of personal information on a website due to a bug in the web code, or a machine fault that results in a document containing personal information being sent to the wrong recipient.
- Examples of a malicious criminal attack include cyber incidents such as phishing, malware or ransomware, brute-force attacks, compromised or stolen credentials. Also, theft of paperwork or data storage devices, or actions taken by a rogue employee or insider threat, as well as social engineering or impersonation.

4. Principles

Through this policy, DPC seeks to give effect to the following foundational principles:

- Personal information is managed with care and respect for individual privacy and in accordance with the IP Act
- Actual or potential harm to individuals is minimised through a proactive and effective approach to data breach response
- Privacy is everyone's responsibility and employees are empowered to identify and report potential data breaches.

5. Proactive readiness for a potential data breach

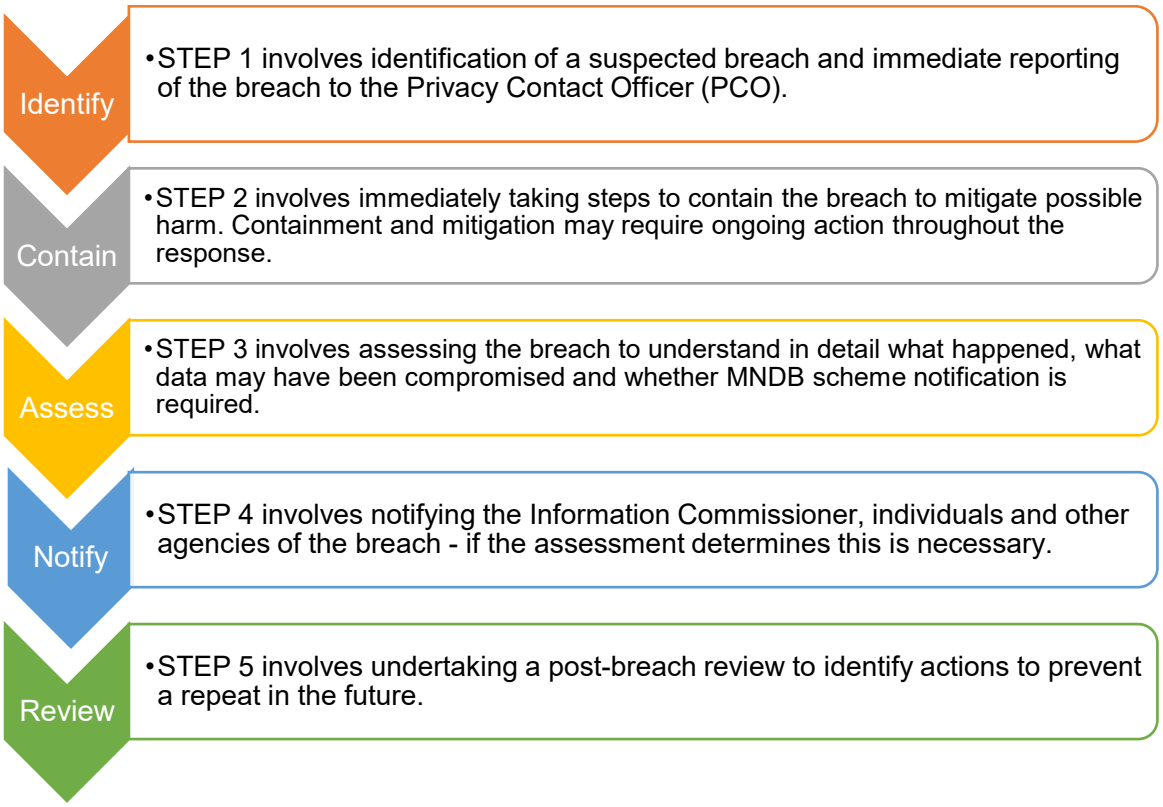
DPC ensures readiness for a potential data breach through the following key proactive steps:

- *Privacy training and awareness* – employees are trained to identify and respond to potential data breaches as part of standard privacy training. Privacy awareness activities are also undertaken throughout the year.
- *Information security measure*s – DPC complies with Information and Cyber Security Policy (IS18).
- *Incident management measures* – DPC prepares and tests incident response policies, playbooks, procedures, systems on a regular basis, including scenarios for a suspected data breach.

- *Third party management* – contracts with third-party service providers generally use Queensland Government terms and conditions that require the third party to comply with parts of the Act as if it were the agency.
- *Policies and procedures* – DPC maintain policies and procedures to ensure swift and coordinated action in the event of a data breach.

6. Data breach response key steps

DPC follows the key steps below when responding to a potential data breach.



STEP 1: Identify the data breach

It is the responsibility of all DPC employees to report a data breach or suspected data breach involving personal information to the PCO immediately. If the employee is unsure whether a breach has occurred, they should err on the side of caution and report the incident.

STEP 2: Contain the data breach and mitigate harm

On receiving information about a suspected data breach, the PCO must conduct a preliminary assessment to ascertain the nature and severity of the breach as this will affect how the breach is triaged and escalated.

DPC will take appropriate steps to contain the breach or reduce its impact and limit any further access or distribution of the affected information. Breach containment and mitigation is an ongoing activity during the response process.

STEP 3: Assess the breach

The PCO must determine if the data breach is an Eligible Data Breach that requires notification to the Information Commissioner, individuals and other agencies under the IP Act.

To determine whether the breach is an Eligible Data Breach, the PCO 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. Both limbs must be met for the breach to qualify as 'eligible.' Regarding the second limb, harm must be both serious **and** likely.

In accordance with the IP Act, the assessment will be conducted as soon as possible but within 30 days, unless DPC extends the assessment period and provides written notice to the Information Commissioner.

STEP 4: Notification

If the data breach is determined to be an Eligible Data Breach, the Information Commissioner must be notified and particular individuals of the Eligible Data Breach in accordance with its obligations under the IP Act.

If DPC becomes aware that an eligible or suspected Eligible Data Breach may affect another agency, DPC will give the other agency a written notice of the data breach in accordance with the IP Act.

STEP 5: Review

After a data breach has been addressed, DPC will review the circumstances of the breach and identify any actions that should be taken to prevent a similar breach in the future. The review will also consider the data breach response process and any required improvements.

7. Register of Eligible Data Breaches

The IP Act requires agencies to keep an internal register of Eligible Data Breaches. If a data breach is assessed to be an Eligible Data Breach, it must be recorded in the DPC Register of Eligible Data Breaches.

8. Legislation

Information Privacy Act 2009

9. Definitions

Term	*Definition*
Data Breach	The IP Act defines a data breach as unauthorised access to, or unauthorised disclosure of, agency information or the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.
Eligible Data Breach	An Eligible Data Breach under the MNDB Scheme occurs when the following are met: (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) 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.
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.
MNDB scheme	Mandatory Notification of Data Breach Scheme is established by Chapter 3A of the *Information Privacy Act 2009* (IP Act), effective 1 July 2025. It requires agencies to notify the Information Commissioner and individuals if it sustains an Eligible Data Breach. A notification must contain certain information set out in the IP Act. It also mandates agencies to take proactive steps to contain, assess, and mitigate data breaches, keep a data breach register, and publish a data breach policy.
Personal Information	The IP Act defines personal information as information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not.
Serious harm	Where the harm arising from the Eligible Data Breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience. Harm to individual can include serious physical, psychological, emotional, financial or reputational harm.

POLICY ADMINISTRATION

1. Monitoring, reporting and management assurance

The Privacy team will monitor the policy as part of the annual legislative compliance process.

2. Communication

This policy will be published on the DPC website and on Compass. Information about the policy will be included in awareness training sessions to be conducted by the DPC Privacy team and in DPC mandatory induction training.

3. Revision History

Please include up to two years' worth of revisions if relevant and ensure previous document is stored in Trim

Revision date	Version Number	Business unit	Description of changes
June 2025	*1.0*	Policy and Legislation	Initial draft

4. Approval

Approval	Date
Executive Governance Group	June *2025*