Office of the Inspector-General of Emergency Management

Data Breach Policy

Version 1.0

Date: July 2025

Contents

Introduction

The Office of the Inspector-General of Emergency Management (the Office) is subject to the provisions of the *Information Privacy Act 2009* (IP Act), which sets out requirements for the fair and responsible collection, use, and management of personal information within the Queensland public sector.

The IP Act requires agencies to notify certain data breaches, publish a Data Breach Policy, and keep a breach register.

The Office is committed to taking actions to prevent data breaches and enhance our ability to respond if they occur. This Data Breach Policy outlines the steps to be taken in the event of a data breach involving personal or sensitive information held by the Office.

Scope

This Policy applies to all Office of the IGEM employees, contractors, and third-party service providers who handle personal or sensitive information. It covers all data breaches, including unauthorised access, disclosure, loss, or misuse of information.

Roles and Responsibilities

Position	Responsibility
Inspector-General	The Inspector-General is responsible for the efficient and proper administration management and functioning of the Office of the IGEM including to ensure that the personal information under the control of IGEM accords with the obligations under the IP Act.
Directors and Executive Managers	Directors and Executive Managers are responsible for: • supporting staff to ensure the Data Breach process is followed and timely advice to the PEO for assessment • ensure employees under their supervision are aware of the requirements of this data breach plan
Principal Executive Officer (PEO) **(In the absence of the PEO, responsibilities will sit with an equivalent level of staff within G&R (AO7), and/or Director)**	The PEO manages the assessment, and will coordinate containment and notification as required for all data breaches that include personal information and is responsible for: • assessment of data breaches containing personal information • notification forms and templates, and central breach register that is used to manage and record details of the incident • coordinating notification of an eligible data breach to the Office of the Information Commissioner (OIC) and affected individuals • educating employees about data breaches and recommending improvement to processes that will reduce the risk of future incidents • reviewing and updating Office of the IGEMs Privacy Policy and this Data Breach Policy.
Employees	All employees, consultants and contractors are responsible for: • recognising a data breach and promptly reporting it • only collecting or using personal information in accordance with the Office of the IGEM Privacy Policy • restricting access to information only to those who require it for their role

	• only keeping information for the length of time necessary in accordance with the retention and disposal schedules • understanding their obligations under relevant legislation, policies, procedures and guidelines, including the Code of Conduct for Queensland Public Service.

Responding to a Data Breach

Outlined below are the steps taken by the Office of the IGEM in response to reported data breaches.

Stage 1: Identify and report

Staff member, contractor or consultant becomes aware of a data breach, or suspects one may have occurred, and immediately reports the incident to the PEO in writing at igem.corro@igem.qld.gov.au.

It is the employee's responsibility to ensure their respective Director and/or Executive Manager is made aware of the written advice in a timely manner.

Where known, the following information should be included in the written advice to the PEO:

- time and date the breach was identified
- how the breach was identified and by who
- who was involved in the breach
- the possible cause and extent of the breach
- the types of personal information involved or suspected to be involved
- a list of affected individuals, or possibly affected individuals
- any action already taken to contain the breach.

Data breaches may be identified by a member of the public who has wrongly received correspondence or who has become aware that they have been affected by a data breach.

Depending on the size and nature of the breach it may be necessary to notify the Incident Manager, Cyber Security Response or the Director, Cyber Security Branch who will be guided by the Queensland Police Service (QPS) Cyber Security Incident Response Plan.

Stage 2: Contain and mitigate

Once a data breach is identified, reasonable steps must be immediately taken to contain the data breach and mitigate the harm caused by the data breach. This may involve:

- searching for and recovering the data
- confirming that no copies were made or that the information was destroyed by the party receiving it
- take appropriate action including, remotely wiping a lost portable device, shutting down impacted computer systems, changing passwords and system usernames. The relevant Director will assess the situation and initiate appropriate actions to contain the breach.

Stage 3: Assess

While taking steps to contain a data breach, the PEO should also assess whether there are reasonable grounds to believe the data breach is an Eligible Data Breach or whether the breach would cause Serious Harm.

In accordance with the *Information Privacy Act 2009 (QLD)*, the assessment will be conducted as soon as possible but within 30 days, unless the Inspector-General extends the assessment period.

The PEO considers the following factors when determining whether **Serious Harm** is likely:

- the kind of personal information accessed, disclosed, or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures, and if so, the likelihood that any of those security measures could be overcome
- the persons, or the kind of persons, who have obtained, or who could obtain, the personal information.
- the nature of the harm likely to result from the data breach
- any other relevant matter. This might include how long the information was exposed, how the breach occurred
- if the breach is considered serious, the Director will brief the Inspector-General, outlining the nature and severity of the breach, the number of potentially affected individuals, actions taken to date, and recommended further steps to reduce harm.

Consider **exemptions** when conducting assessment: Refer to the *IP Act 2009* (Qld), Part 3A, Part 3. There are specific exemptions that may apply during a data breach assessment.

Stage 4: Notify

Where it is confirmed that an eligible data breach has occurred, the Inspector-General and the individual affected by the breach will be notified, unless an exemption applies.

The PEO will report to OIC by completing an online Privacy Breach Report via: OIC Agency Portal | Office of the Information Commissioner Queensland.

Depending on the circumstances of the breach, the Office may also notify other organisations, such as the QPS.

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

Stage 5: Update Register of eligible data breaches and record keeping

The Office of the IGEM maintains appropriate data breach records to provide evidence of how known and suspected data breaches are managed. This includes a **register of eligible data breaches**, as required under section 72 of the IP Act. The PEO will maintain the register and ensure it is updated to reflect each data breach.

Stage 6: Review post-data-breach and remediate

Review and analyse all aspects of the breach to identify causes and determine actions or strategies to prevent similar breaches from reoccurring. The review may include evaluating:

- the Office policies
- delivering a Data Breach awareness session to staff members
- contracts and whether contractual obligations were met in response to the incident
- ICT systems, including security measures and system functions to enable containment and mitigation actions
- how this Policy functioned during the response to the breach.

Appendix A: Related policy and supporting documents

Legislation

- *Code of Conduct for the Queensland Public Service*
- *Public Sector Act 2022*
- *Public Records Act 2023*
- *Right to Information Act 2009*
- *Information Privacy Act 2009*

Policy

- Privacy Policy

Appendix B: Key Definitions

Concept	Definition
Personal information	Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion
Data breach	A 'data breach' means either of the following in relation to information held by IGEM: • unauthorised access, or unauthorised disclosure of the information. • the loss of the information in circumstances where unauthorised access to, or unauthorised access disclosure of the information is likely to occur.
Eligible data breach	For a data breach to be assessed as an 'eligible data breach', both of the following must apply: • 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').
Unauthorised access	Unauthorised access to personal information occurs when information held by an agency is accessed by someone who is not authorised to do so.
Unauthorised disclosure	Unauthorised disclosure occurs when an agency intentionally or unintentionally discloses personal information when the agency does not have permission or is not entitled to make that disclosure.
Loss	Loss of personal information involves an agency no longer having possession or control of the information.
Serious harm	Serious harm is defined in schedule 5 of the IP Act as: • 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.
Exemption from notification	Exemptions are set out in section 55-60 of the IP Act 2009 Information Privacy Act 2009

Appendix C: MNDB Scheme assessment tool

This tool is designed to help Queensland government agencies determine whether a data breach qualifies as an eligible data breach under section 47 of the *IP Act 2009*. It provides a structured framework for conducting the assessment, along with guidance and considerations at each step of the process.
Mandatory Notification Data Breach (MNDB) scheme assessment tool