

Policy number	GOV-005 2024 PR2
eDocs	239703
Type	Procedure
Status	Final
Classification	Public

Data and privacy breach procedure

Version: 3 | Date effective: 1 July 2025 | Review date: 1 July 2026

Audience

All staff, including contractors and volunteers.

Purpose

This procedure provides information about the process for responding to a data and/or privacy breach and the tasks and responsibilities to be undertaken to comply with the *Data and Privacy Breach policy*.

Application

This procedure applies in any circumstance where a data and/or privacy breach is suspected or confirmed.

Responsibilities

The following officers have responsibilities in implementing the *Data and Privacy Breach policy* and this procedure:

Officer	Responsibilities
Deputy Ombudsman	<ul style="list-style-type: none"> member of the Emergency Response Team (ERT) for major data/privacy breaches (except breaches involving DSU) oversee response to major data/privacy breach report to Ombudsman on major data/privacy breach response
Director, DSU	<ul style="list-style-type: none"> member of the ERT for major data/privacy breaches involving DSU oversee response to major data/privacy breach report to Ombudsman on major data/privacy breach response
Executive Director, Corporate Strategy	<ul style="list-style-type: none"> member of the ERT for major data/privacy breaches report to Ombudsman, ELT and SMT on major data/privacy breach response
General Counsel	<ul style="list-style-type: none"> convene and chair ERT meetings for major data/privacy breaches consult with Advisor, RTI/IP and provide legal advice and review concerning the management of minor data/privacy breaches identify legal obligations and provide advice

Principal Officer, Information Services	<ul style="list-style-type: none"> • member of ERT for major data/privacy breaches • establish the cause and impact of a data breach involving ICT systems • manage containment of IT systems where relevant including monitoring for recurring incidents • engage external IT security consultants or forensic specialists if the breach requires advanced analysis or response • recommend technical or procedural changes to prevent future breaches based on lessons learned • maintain detailed documentation of the breach response process, including actions taken, systems affected, and any recommended follow-ups or changes to ICT policy
Advisor, Right to Information and Privacy	<ul style="list-style-type: none"> • assess breaches and suspected breaches in consultation with the General Counsel • determine action to be taken following assessment • primary responsibility, in consultation with the General Counsel, for managing all aspects of minor data/privacy breaches, • member of the ERT for major data/privacy breaches • coordinate ERT and provide support to members • provide privacy advice
Senior Communication Officer	<ul style="list-style-type: none"> • member of the ERT for major data/privacy breaches • assist in communicating with the media and external stakeholders • prepare media releases
HR Manager	<ul style="list-style-type: none"> • member of the ERT for major data/privacy breaches where the breach involves the personal information of staff or where it may lead to disciplinary action • provide advice where the breach involves the personal information of staff or where the incident may lead to disciplinary action of a member of staff
All staff	<ul style="list-style-type: none"> • notify their manager if they identify a data and/or privacy breach or a suspected data and/or privacy breach

Requirements

Data and/or privacy breaches

Data breaches and privacy breaches can occur for a variety of reasons including:

- human error
- misconduct by an employee
- malicious activity by an external party.

Human error

Examples of breaches due to human error include:

- loss of a laptop, USB or paper records that contain personal information held by the Office (e.g. left on a train or bus, stolen in home break-in)
- accidental disclosure of personal information (e.g. sending an email to the wrong addressee).

Misconduct

Examples of breaches due to misconduct include:

- inappropriate or fraudulent use of an Office database containing personal information
- intentional disclosure of complainant's personal information or confidential complaint information other than in accordance with legislation and policy.

Malicious activity

Examples of breaches due to malicious activity include:

- scams that trick you into releasing personal information
- malware attacks (an umbrella term that refers to a range of different types of computer system security breaches) including:
 - trojan horse – program that appears as a typical file but hides malicious behaviour
 - ransomware – malware virus that blocks access to data until a 'ransom' is paid
- password attacks (a hacker guesses a password to gain access to a computer system)
- denial-of-service (DoS) attacks (attempts to knock a network or service offline by flooding it with traffic to the point the network or service can't cope)
- distributed-denial-of-service (DDoS) attacks (hijacking a device, often using botnets, to send traffic from multiple sources to take down a network)
- man-in-the-middle attacks (a hacker compromises another entity's system to launch an attack on Office servers, either by sneaking through an already established connection, or stealing another entity's IP address and disguising themselves as that entity)
- Office premises broken into and ICT equipment and/or hard copy documents stolen.

Process

The following process will be implemented to respond to a data and/or privacy breach:

- Identify that a breach has occurred
- Contain the breach
- Assess the breach
- Evaluate the risks associated with the breach
- Make required/appropriate notifications
- Prevent future breaches

Identify that a breach has occurred

- QO may become aware of a breach via a privacy complaint (see *Privacy complaint procedure*), or it may be identified internally by staff.
- Any staff member who becomes aware of an actual or suspected data and/or privacy breach (either through a complaint or through other means) must report it as soon as possible to their manager.
- The manager must inform the Advisor, RTI/IP or General Counsel.
- The manager must ensure that any process that may be the cause of the data and/or privacy breach is discontinued. Staff responsible for the process that may be the cause of the incident, should suspend implementing that process until further advised by the manager.
- The Advisor, RTI/IP must report the breach to the General Counsel, the Executive Director, Corporate Strategy and the Deputy Ombudsman or Director, DSIU.
- If the breach is identified in a complaint or information received from a person/s impacted, the Advisor, RTI/IP will acknowledge the complaint within five working days in accordance with the *Privacy complaint procedure*.

Contain the breach

Steps should be immediately taken by the relevant manager, in consultation with the Advisor, RTI/IP and/or General Counsel, to contain the breach and to mitigate actual or potential harm from the breach. For example:

- stop unauthorised access
- recover any records
- shut down the system that was breached.

If the breach involves electronic records held on an ICT system, in consultation with the Principal Officer, Information Services, the following steps may be appropriate:

- isolate the cause/s of the breach in the relevant system, software or database
- shut down the compromised system, software or database, or if not practical to shut down the system, revoke or change access privileges
- reset log-in details and passwords for compromised devices, systems or databases
- quarantine any compromised devices.

If the breach involves the loss of a device or physical files, the following steps may be appropriate:

- arrange to have the lost device remotely disabled
- arrange a search of the site where the loss occurred by contacting any relevant authorities (e.g. public transport operator, airline)

If the breach involves the unauthorised disclosure of personal information to a third party by email, the following step may be appropriate:

- recall the email from the recipient and ask the recipient to delete the email and notify the Office that they have done so

If the breach involves the unauthorised disclosure of personal information to a third party by post, the following step may be appropriate:

- contact the recipient and ask them not to open or read the posted materials, and arrange for collection/return of the posted materials.

Assess the breach

The Advisor, RTI/IP, in consultation with the General Counsel (for legal advice and review), will assess the breach or suspected breach to determine if it should be categorised as a major data breach (the breach involves personal information and is likely to result in serious harm to an individual). This is called an 'eligible data breach' under the IP Act.

Serious harm to an individual includes, for example, serious physical, psychological, emotional or financial harm or serious harm to the individual's reputation.

The assessment must be completed as soon as possible but no later than 30 days of becoming aware of the breach.

The assessment may include use of OIC's assessment tool, that is available on its website.

In determining whether there is serious harm, the following factors may be considered:

- 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 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.

A record will be kept of the assessment and will include:

- the factual background to the matter
- when the breach occurred
- the cause and extent of the breach
- how the breach can be further contained (if it has not already addressed); and
- preliminary recommendations for changes to practices, procedures and systems.

Once the assessment is completed, the Advisor RTI/IP may:

- resolve the matter at the assessment stage (only appropriate if it is not a major data breach) (and advise the Executive Director, Corporate Strategy and the Deputy Ombudsman or Director, DSU that this has occurred)
- refer the matter to ERT by notifying the General Counsel (if it is a major data breach, or there are other significant concerns about the matter).

The urgency for referral to ERT is to be assessed by the Advisor RTI/IP or General Counsel on a case-by-case basis. However, in most cases, a major data breach should be referred within 24 hours.

Resolution

If the matter is not required to be referred to ERT, it may be resolved by the Advisor RTI/IP, in consultation with General Counsel (for legal advice and review):

- If the data or privacy breach was notified as a result of a complaint, part of the resolution must involve an outcome letter to the complainant (see *Privacy complaint procedure*). This outcome letter should be sent within 45 business days after receipt of the complaint (except if an extension is requested from the complainant).
- The Advisor, RTI/IP will determine whether notification of impacted individuals is required, including consideration of the following:
 - whether notification will assist in demonstrating a commitment to QO's privacy obligations and an open and transparent governance
 - whether notification will help to avoid or lessen the damage by enabling the individual to take steps to protect themselves
 - the risk of harm to the individual
 - whether, if the individual were a vulnerable member of the community, for example a victim of family or domestic violence, the risk of harm would change
 - the ability of the individual to take further steps to avoid or remedy harm
 - whether the information is sensitive, or likely to cause humiliation or embarrassment to the individual; and
 - other relevant legislative requirements, such as secrecy or confidentiality obligations.
- There are occasions where notification to an affected individual can be counterproductive. For example, notifying individuals about a technical privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant data breach.
- If the person is notified, they should be advised of their entitlement to make a complaint under the *Privacy complaint procedure*.

- In dealing with a privacy breach the QO's response may include:
 - an apology
 - an explanation of what happened and steps that are being taken to prevent it from recurring;
 - an undertaking not to repeat the action constituting the breach
 - practical assistance to deal with the consequences of the breach.
 - a change to work responsibilities, systems, practices, policies, or procedures

Emergency Response Team

Where a data and/or privacy breach is assessed as a 'major breach', an Emergency Response Team (ERT) will be convened by the General Counsel, to manage the response to the breach.

The ERT will comprise:

- Deputy Ombudsman and/or Director, Detention Services Inspection Unit (as appropriate)
- Executive Director, Corporate Strategy
- General Counsel
- Principal Officer, Information Service
- Advisor, Right to Information and Privacy
- Senior Communication Officer
- HR Manager (where the breach involves the personal information of staff or where the incident may lead to disciplinary action involving a member of staff)
- Any other member/s of the SMT, as determined by the Ombudsman, who can assist in the management of the breach.

The ERT will develop a plan for responding to the breach, and take the action necessary to implement the plan. The ERT may:

- immediately contain the breach and minimise the harm (if not already addressed)
- arrange for an audit to identify the type of information involved and/or the extent of the breach
- determine if and how affected people will be notified and what information they will be provided
- ensure people affected by the breach are contacted where appropriate
- consider whether it is necessary to set up a 'hot line' to take calls from people who may have been affected by the breach
- determine which stakeholders will be notified, and arrange for this to occur
- provide information requested by the Information Commissioner
- document the response to the data breach; and
- conduct a review of the response.
- decide any further steps to be taken to resolve the matter (see resolution)

The ERT will produce a report at the conclusion of the process, for submission to the Ombudsman and the Audit Committee.

Evaluate the risks associated with the breach

Once the breach is contained, the ERT will conduct a risk assessment, including considering:

- what system has been compromised?
- who is affected?
- what information is involved (contact details, email addresses, financial information)?
- what is the source of compromise, and the timeframe involved?

- what parties have gained unauthorised access to the information?
- what harms (to affected persons) could potentially be caused by the breach (financial, reputational, embarrassment)?
- how could the information be used to cause foreseeable harm to affected persons (identity theft, financial loss, humiliation)?
- does the breach indicate a systemic problem with the Office's practices and procedures?
- have any laws have been contravened by the data breach (e.g. s 92 of the *Ombudsman Act 2001*, or s 30 of the *Inspector of Detention Services Act 2022*)?
- what is the reputational damage to the Office?
- what is the Office's legal liability?

The Office's Risk assessment framework may be adapted to undertake and record the risk assessment.

The ERT may review and/or amend the response plan in light of the risk assessment.

Make required/appropriate notifications

ELT will consider what notifications are required, as set out below (taking into account any exemptions that apply in the IP Act)

Notify the Office of the Information Commissioner

In the event of a major privacy breach the OIC must be notified as soon as practicable following the breach. The Advisor RTI/P prepares the notification in consultation with General Counsel.

The notification to the OIC must include:

- the contact details of a QO officer
- the date the breach occurred
- if relevant, the period during which the access or disclosure was available or made
- a description of the breach
- information about how the breach occurred
- steps the Office has taken or will take to contain the breach and mitigate the harm caused to individuals
- a description of the kind of personal information the subject of the data breach, without including any personal information in the description
- the Office's recommendations about the steps individuals should take in response to the data breach
- the total number (or if not known, an estimate) of:
 - individuals whose personal information has been accessed, disclosed or lost
 - individuals likely to suffer serious harm
 - individuals notified of the data breach
- whether the individuals notified have been advised about how to make a privacy complaint to the Office.

The OIC can provide advice on responding to the breach. Notification also assists OIC to respond to community enquiries about the breach.

Notify Individuals

In the case of a major data breach, if it is reasonably practicable to notify each individual whose personal information has been accessed, disclosed or lost, or otherwise affected by the breach, the

Office must take reasonable steps to do so. If this is not practicable, the Office must take reasonable steps to notify each individual likely to suffer serious harm. The notification to each individual must include:

- the contact details of an officer the individual can communicate with about the breach
- the date the breach occurred
- if relevant, the period during which the access or disclosure was available or made
- a description of the breach
- a description of the personal information involved
- information about how the breach occurred
- recommendations about the steps the individual should take in response to the breach
- steps the Office has taken or will take to contain the breach and mitigate the harm caused to individuals
- information about how an individual may make a privacy complaint to the Office.

If the process commenced with a complaint, EMT must ensure that a response to the complaint is provided to the complainant within 45 business days in accordance with our *Privacy complaint procedure*.

Publication of a Notice

In the case of a major data/privacy breach, if it is not reasonably practicable to personally contact the individuals likely to suffer serious harm, the following information should be published on the Office website for a period of at least 12 months:

- the contact details of an officer the individual can communicate with about the breach
- the date the breach occurred
- if relevant, the period during which the access or disclosure was available or made
- a description of the breach
- a description of the of the kind of personal information involved without including any personal information in the description
- information about how the breach occurred
- recommendations about the steps the individual should take in response to the breach
- if relevant, the period during which the access or disclosure was available or made
- steps the Office has taken or will take to contain the breach and mitigate the harm caused to individuals
- information about how an individual may make a privacy complaint to the Office.

The Office must notify the OIC of the publication of the notice and how it can be accessed as soon as practicable.

Other notifications:

ERT will consider whether any other notifications may be required, for example to:

- other agencies that may be affected by the data breach

-
- Office of the Australian Information Commissioner (OAIC) (if the data breach involved Tax File Numbers (TFN)).¹
 - Queensland Government Information Security Virtual Response Team (refer to the *Information security policy* (IS18:2018) and QGEA Information security incident reporting standard)
 - Queensland Police Service (where the data breach is suspected to involve a criminal offence)
 - Crime and Corruption Commission (where there is a reasonable suspicion of corrupt conduct)
 - Queensland Parliamentary Justice, Integrity and Community Safety Committee
 - Queensland Attorney-General
 - media (ERT should coordinate with the Senior Communications Officer in relation to media releases, requests and alerts).

If the data breach involves suspected misconduct the matter should be managed under the Office's Code of Conduct.

Prevent future breaches

The ERT will consider what short or long-term measures may be taken to prevent any reoccurrence of the breach.

If breach was caused by an employee, ERT will consider whether the Office should:

- provide additional staff training, reminders or information
- improve oversight or supervision of staff
- enhance auditing or monitoring
- review or amend policies or procedures
- introduce new controls or restrictions on system access.

If the breach was caused by a third party, ERT will consider whether the Office should:

- improve ICT or building security
- apply additional security protections (e.g. encryption)
- give additional or different guidance to staff or contractors
- amend access arrangements.

Registering and reporting data/privacy breaches

The Advisor, RTI/IP will maintain a register recording all data/privacy breaches. For major data/privacy breaches the register must include:

- that the breach was assessed as a major data/privacy breach
- a description of the data/privacy breach
- the names of individuals notified, and the date and method used to notify them
- steps taken to contain the breach and mitigate the harm caused by the breach
- the date that a statement was provided to the OIC and when further information was provided
- details of any exemption relied upon
- actions taken to prevent future data/privacy breaches of a similar kind.

¹ There is a notifiable data breach scheme that applies in relation to Tax File Numbers (TFN) under the *Privacy Act 1988* (Cth). If the breach involves TFNs, it should be reported to the Office of the Australian Information Commissioner (OAIC) using its Notifiable Data Breach Form.

The ERT will prepare a report on each major data/privacy breach for submission to the Ombudsman and the Audit Committee.

Definitions

Term / Acronym	Definition
Advisor, RTI/IP	Advisor, Right to Information and Privacy
Data breach	A data breach occurs when Office information is subject to unauthorised access, unauthorised disclosure, or loss (in circumstances where unauthorised access or disclosure is likely to occur from the loss).
DSIU	Detention Services Inspection Unit
ELT	Executive Leadership Team
ERT	Emergency Response Team
ICT	Information and communication technology
IP	Information Privacy
IP Act	<i>Information Privacy Act 2009</i>
IPPs	Information Privacy Principles
Major data/privacy breach	A data/privacy breach that involves personal information, and it is likely to result in serious harm to an individual to whom the personal information relates. This means the same as an eligible data breach under Chapter 3A of the IP Act.
Manager	Member of the Senior Management Team or person who supervises/manages other staff
Office	Office of the Queensland Ombudsman
Ombudsman	Queensland Ombudsman and Inspector of Detention Services
Privacy breach	A privacy breach occurs when personal information is accessed, used or disclosed without authorisation, or is lost, or otherwise dealt with in a way that would not comply with the <i>Information Privacy Act 2009</i> .
RTI	Right to Information
OAIC	Office of the Australian Information Commissioner
Office	Office of the Queensland Ombudsman
OIC	Office of the Information Commissioner
Ombudsman	Queensland Ombudsman and Inspector of Detention Services
QGEA	Queensland Government Enterprise Architecture

SMT	Senior Management Team
------------	------------------------

Policy documents

Related policy documents:

- GOV-005 2024 P *Data and privacy breach policy*
- GOV-005 2024 PR1 *QPP privacy policy*

Related documents

- *Ombudsman Act 2001 (refer to s 92)*
- *Inspector of Detention Services Act 2022 (refer to s 30)*
- *Information security policy (IS18:2018)*
- *QGEA Information security incident reporting standard*
- *ICT Incident Management Policy and Procedures*
- *Complaints Management System Policy*
- *Prevention and management of fraud and corruption policy and procedure*

Policy owner

General Counsel

Approval

Action	Officer	Date
Author	Alex Andrews Advisor, Right to Information and Privacy	19 / 2 / 2025
Endorsed	Christine Jones General Counsel	25 / 2 / 2025
Approved and authorised for external publication	Anthony Reilly, Queensland Ombudsman and Inspector of Detention Services	25 / 2 / 2025

Document control

Version	Amendment history	Date
1	Draft	13 / 02 / 2025
2	Final	25 / 02 / 2025
3	Amendments to implement legislative changes made by the <i>Information Privacy and Other Legislation Amendment Act 2023</i> , coming into force on 1 July 2025.	1 / 7 / 2025