Plan

# Privacy Data Breach Response Plan

**Version:** 2.0 | **Version effective date:** 1/7/2025
**Supersedes:** Privacy Data Breach Response Plan 1.0

## Purpose and scope

This Plan applies to individuals who have had the Queensland Public Trustee (QPT) collect and handle their personal information. It includes all QPT employees and volunteers (whether permanent, part-time, full time, casual or contractors) and customers who may have concerns about the way QPT deals, or has dealt, with their personal information.

Queensland Public Trustee (QPT) has obligations under the *Information Privacy Act 2009* (Qld) (IP Act) and other related legislation to protect the personal information that it holds. The IP Act establishes the Queensland Privacy Principles (QPPs) that QPT must comply with when collecting, managing, using or disclosing personal information, and sets out what QPT must do if a privacy data breach occurs in relation to the personal information it holds.

The Privacy Data Breach Response Plan outlines the steps QPT will take to contain, mitigate, assess and respond to a breach, including to eliminate or minimise the risk of harm that might arise from a breach. Swift action is crucial to the success of the response.

This Plan is intended to help employees and contractors understand the process and the roles, responsibilities and clear lines of authority that apply in the event of an actual or suspected privacy data breach, regardless of whether a complaint has been received.

How to respond to privacy data breaches as set out in this Plan applies to all QPT employees and volunteers (whether permanent, part-time, full time, casual or contractors).

## Overview

### What is a privacy data breach?

A privacy data breach occurs when there is:

- unauthorised access to, or unauthorised disclosure of, personal information held by QPT, or
- a loss of personal information held by QPT in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

A breach may be deliberate or accidental. It can occur as result of a range of circumstances, for example, technical issues, human error, failure of information handling or security systems, inadequate training, misunderstanding of the law, or through a malicious or deliberate act. Some examples of privacy data breaches that might occur within QPT include:

- theft of a document or part of a document that contains personal information (for example, downloading personal information from a QPT database, or taking copies of files without permission)

- accidentally sending personal information to the wrong person (for example, sending an email to the wrong recipient or posting documents to an incorrect address)
- disclosing personal information to a third party who does not have a legal right to it (for example, sharing an individual's personal health information with someone else because they are a concerned friend)
- using QPT's information systems to find personal information for a non-work-related purpose (for example, accessing the QPT customer file of a friend or relative to find out information about them, or accessing payroll information to find out another employee's contact details to invite them to a social event)
- leaving a file that contains personal information in an unsecured location where someone else is able to access it (for example, leaving a document on public transport, or leaving a computer screen unlocked when not at your desk so that others can view the information)
- personal information being compromised during a cyberattack and intentionally accessed by a person external to QPT
- a database hosted in a cloud environment or a web facing application containing personal information not having appropriate access controls and personal information in the database is visible and accessed by unauthorised individuals.

### Information Privacy Framework

QPT's Information Privacy Framework is the collection of policies, procedures and tools that QPT uses to manage information privacy appropriately, and to investigate and resolve information privacy breaches and customer complaints regarding information privacy, when these occur.

The Information Privacy Framework includes the Information Privacy Complaints Management Policy and Information Privacy Complaints Management Procedure, which set out the legislative frameworks, core principles and procedures for managing information privacy complaints. Typically, an information privacy complaint is made by:

- a QPT customer or other person external to QPT following them becoming aware that there may have been an information privacy breach.
- a QPT employee where they believe QPT has not dealt with their personal information in accordance with the QPPs.

The Framework includes QPT's internal Privacy Breach Register where all reported information privacy complaints and privacy data breaches must be recorded.

### Business Continuity

Sometimes a privacy data breach occurs that impacts multiple people or systems, and/or causes disruption to the continuous delivery of an organisation's activities or services.

In the event of such a breach, QPT has a suite of other response plans in place that may be activated in conjunction with this Privacy Data Breach Response Plan to manage and respond to the breach, and to

ensure the prompt recovery, resumption and restoration of QPT's systems. These other plans include QPT's Crisis Management Plan, Business Continuity Plan and IT Disaster Recovery Plan.

More information about how to assess the level of impact of a privacy data breach and when a breach may need to be managed in conjunction with another response plan, is provided in the 'Handling privacy data breaches' section of this document.

### Information Security Management

QPT's Information Security Management Framework defines the organisational system that supports implementation of information security across QPT. Key aspects of the Information Security Management Framework include protection of information assets; management of information security threats and risks to QPT, its staff and customers; and detecting and preventing unauthorised access to information held by QPT.

## Handling privacy data breaches

QPT's approach to managing privacy data breaches is aimed at containing the breach, assessing the likelihood of the risk of harm and mitigating the risk of harm caused, or potentially caused, by the breach, and taking all reasonable steps to prevent similar breaches from occurring again.

There are six steps involved in managing a privacy data breach, and the actions required under each of these steps is explained in more detail below. (Refer to Appendix A - Privacy Data Breach Flowchart).

1. **Identify** the breach
2. **Report** the breach
3. **Contain** the breach
4. **Assess** and **mitigate** risks
5. **Consider notification** to affected individuals and the Office of the Information Commissioner
6. **Review** to prevent future breaches

**Wherever possible, these steps are to occur simultaneously or in quick succession.** Depending upon the circumstances of the breach, not all steps may be necessary, or some steps may be combined. For example, not all steps may be necessary where an individual advises QPT that they have received personal information belonging to another person in error and returns that information to QPT at the same time. With some breaches however, it may be appropriate and necessary to take all the steps depending upon the specific nature and extent of the breach.

The Manager or Nominated Officer (a person within the organisational unit nominated by QPT's Compliance Systems and Governance (CSG) unit), is to investigate the actual or suspected breach when an information privacy complaint is received, or an actual or suspected breach is discovered, and is required to provide regular updates to CSG regarding the investigation and any action/s planned or taken.

Breaches must be dealt with on a case-by-case basis and must include undertaking an assessment of the likelihood of the breach resulting in harm to the individual(s) affected by the breach to decide the appropriate course of action. Depending on the likelihood of the breach resulting in harm and the seriousness of that harm, it may be necessary for a Privacy Data Breach Response Team to be stood up to further handle the

breach. The Executive Director, Strategy and Governance decides whether a Privacy Data Breach Response Team is required and who it will include. (Refer to Appendix B to find out more about the role, responsibilities and expected actions of a Privacy Data Breach Response Team).

During the investigation of a breach, **it is important for the Manager or Nominated Officer to immediately inform the Director, Compliance Systems and Governance should they know, or reasonably suspect, that the breach has caused or poses a risk of serious harm to an individual affected by the breach.** Immediate notification is necessary to ensure QPT complies with the legislated timeframe for notifying the Queensland Office of the Information Commissioner (OIC) of breaches that have caused or pose a risk of serious harm.[1]

## 1. Identify the breach

There are generally three ways in which a privacy data breach or suspected breach may be identified. These are:

- Internal identification: Where a QPT employee or contractor notices personal information has been inappropriately released to a third party, been inadvertently made public, or has been lost or stolen. For example, where:
  - an individual's personal information has been provided to a third party who is not the intended recipient.
  - it was intended for de-identified information to be provided for statutory reporting purposes, but the information sent has personal identifiers included.
  - during a routine software update, the person performing the update notices the unintended momentary publication of customer records containing personal information on the internet.
  - an employee accidentally leaves a device containing personal information on public transport.
  - a device containing personal information is stolen from QPT premises or an employee's home.
- External identification: Where a third party receives, or is made aware of the release of, an individual's personal information and notifies QPT. For example, where:
  - a trusted third party with secure recordkeeping processes (for example, another government department, public guardian, contracted supplier, etc.) contacts QPT to advise they have received someone's personal information in error.
  - another organisation, such as a payroll vendor, notifies QPT that their systems have been compromised and that the personal information of employees may have been released.
- Affected individual identification: Where a QPT customer or employee identifies that their personal information appears to have been released to a third party without their permission and lodges a complaint.

[1] Under the mandatory notification of data breach scheme in the *Information Privacy Act 2009* (Qld), where QPT does not know, but reasonably suspects that a privacy data breach is an 'eligible data breach' i.e. a breach may have caused or poses a risk of serious harm to an individual to whom the personal information relates, QPT must assess whether there are reasonable grounds to believe the breach is an 'eligible data breach' within 30 days (unless QPT is satisfied it will not be able to complete the assessment in 30 days and it has started the assessment and given the OIC written notice of the extended time). Where QPT knows or reasonably believes that the breach is an 'eligible data breach', QPT must as soon as practicable notify the OIC and the affected individuals.

## 2. Report the breach

When an actual or suspected privacy data breach has occurred, the QPT employee or contractor who identified or received information about the breach must immediately report it to their QPT Manager. For staff in a regional office, this means the Regional Manager, and for all other staff their direct line manager.

The Manager contacts CSG to advise an actual or suspected privacy data breach has occurred.

Where known, the following information should be included in the report:

- the time and date the breach was discovered or reported to QPT
- who was involved in the breach
- how the breach was discovered and by whom
- the possible cause and extent of the breach (this may not be fully known at this time)
- the type(s) of personal information involved or suspected to be involved
- a list of affected individuals, or possibly affected individuals
- the likelihood and consequence of harm to those individuals whose personal information is involved in the breach
- the likelihood and consequence of other types of harm (for example, harm to QPT's reputation)
- any action/s already taken to contain the breach, including actions to mitigate the likelihood or consequence of harm.

CSG will add the details of the breach into QPT's internal Privacy Breach Register and, if required, will provide advice and support to the Manager to ensure the breach is handled appropriately.

If the breach has been reported as part of a complaint, CSG will identify a Nominated Officer within the relevant organisational unit to gather information and investigate what has occurred. This will usually be the Manager of the organisational unit involved, but may be another staff member with sufficient experience and seniority to investigate the matter.

If the breach appears to involve fraud or corruption, CSG or the Manager must contact QPT's Ethics and Integrity Unit to ensure the matter is considered in accordance with the Fraud and Corruption Control Policy.

## 3. Contain the breach

As soon as a Manager receives a report that a privacy data breach has occurred, they must immediately, and continue to, take all reasonable steps to contain the breach.

Depending on how the breach occurred, this could include:

- stopping a staff member from continuing an activity or suspending the activity that led to the breach
- making efforts to recover the personal information, including seeking to recover personal information in the possession of an unintended third party[2]

[2] Where a third party is in possession of the personal information and declines to return it, it may be necessary to seek advice from the Legal Services unit on what action can be taken to recover the information.

- contacting the Information and Technology unit to arrange for a system to be locked down or for system access to be revoked or changed
- addressing a weakness in physical security.

Priorities and risks should be initially, and continually, assessed based on what is known at each point in time. Managers should consider the following to help them to identify appropriate containment strategies:

- How did the breach happen?
- Is the information still being accessed, disclosed or lost?
- Who has access?
- What can be done to secure the information?
- What can be done to reduce the risk of harm? (Further information is provided in the 'Assess and mitigate risks' section of this document).

For example, if an officer has accidentally sent an email containing personal information to the wrong recipient, they may be able to successfully recall the email, or contact the recipient to confirm that they have deleted the email from their system and that no copy has been taken. When deciding what containment action is appropriate, Managers should have regard to the adequacy of containment methods involving electronic data breaches e.g. is deletion sufficient if it could have been forwarded or backed up elsewhere?

Managers should take steps to preserve any evidence that may be valuable in determining the cause of the breach or allowing QPT to take corrective action.

## 4. Assess and mitigate risks

While taking steps to contain a privacy data breach, the Manager or Nominated Officer, should also take steps to mitigate the likelihood and consequence of harm to those individuals whose personal information is involved in the breach. This will require the Manager or Nominated Officer gathering all necessary information to make an assessment as to the likelihood and consequence of harm that might occur as a result of the breach. This assessment must include consideration of the following, together with any other relevant matters given the circumstances of the breach:

- the kind of personal information accessed, disclosed or lost. For example, where a breach involves identification credentials or documents (such as passports, driver licences, etc), or credit card or bank account details, there is a heightened risk of harm from identify theft, fraud or financial crime
- the sensitivity of the personal information. For example, breaches involving sensitive information generally have a higher likelihood of resulting in serious harm[3]

[3] Sensitive information is defined in Schedule 5 of the *Information Privacy Act 2009* (Qld) to include racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information that is not otherwise health information, biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or biometric templates.

- whether the personal information is protected by one or more security measures. For example, where information is lost but security measures are in place, such as encryption or a strong password, these are more likely to prevent unauthorised access or disclosure of the information
- if the personal information is protected by one or more security measures, the likelihood of those measures being overcome. For example, if the encryption technique used is robust, or the password is sufficiently complex that it would take many years to crack, the likelihood of harm may be reduced
- the persons, or kinds of persons, who have obtained, or who could have obtained the personal information. For example, where there is unlawful intent or motive of those with access to the information, or if there a relationship between the individual whose personal information is affected and the recipient of that information, the likelihood of harm may be increased
- the nature of the harm likely to result from the breach. For example, is the harm likely to be serious, such as financial loss, identity theft, emotional harm, reputational damage, physical or personal safety harms, domestic and family violence related harms, or a combination of these.

Depending upon the circumstances of the breach, it may also be necessary for the Manager or Nominated Officer to also consider:

- whether a combination of different types of personal information is involved that may lead to an increased risk of harm
- how long the information has been exposed or affected by the breach, including the amount of time the information was exposed prior to the breach being discovered
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm
- actions already taken to reduce the risk of harm.

**Is there potential for 'serious harm'?**

In assessing the likelihood and consequence of harm that could result from the breach, if the Manager or Nominated Officer at any point during their assessment reasonably suspect that the breach has or could result in **serious physical or personal safety, psychological, emotional, financial or reputational harm to an individual because of the breach,** the Manager or Nominated Officer must notify the Executive Director, Strategy and Governance immediately (by phone where possible), including with as much information as possible about what has occurred, the known causes or impacts, and actions taken so far. The Manager or Nominated Officer should also make their own Director and Executive Director aware that a privacy data breach may have caused or poses a risk of serious harm that has been notified to the Executive Director, Strategy and Governance which may need to be reported to the OIC. Managers and Nominated Officers should use the OIC Mandatory Notification of Data Breach (MNDB) assessment tool to assist with their assessment of the breach and the requirement to notify the Executive Director, Strategy and Governance, keeping a record of their assessment.

The Executive Director, Strategy and Governance, will assess all information available and decide whether a privacy data breach may have caused or poses a risk of serious harm where the likelihood is **more probable than not**. Where this is the case, the Executive Director, Strategy and Governance will stand up a Privacy Data Breach Response Team to take over the investigation and handling of the breach and actions required under

Steps 5 and 6. Appendix B contains information about the role and responsibilities of the Privacy Data Breach Response Team.

Examples of when harm may be **serious** include:

- **physical or personal safety** – serious harm may occur if an affected individual's safety is at risk or there is a risk of physical harm occurring. This may arise where a person's home or work address has been disclosed, and due to the person's occupation or association with others, they become more susceptible to the risk of physical harm or being the victim of stalking, harassment or domestic and family violence.
- **psychological or emotional** – serious harm may occur if sensitive information of an individual is disclosed that may lead to distress and embarrassment, such as health information.
- **financial** – serious harm may occur if an affected individual could become the victim of identity theft or fraud, losing money and other assets. Serious harm could also arise where the individual incurs costs of responding to a breach, such as reissuing identity documents or needing to engage the services of professionals to assist with legal, psychological or medical issues arising from the breach.
- **reputational** – serious harm may result from an affected individual experiencing reputational damage from information which may negatively impact social status or a person's professional or business reputation.

Where a Manager or Nominated Officer do not have any suspicion that there is a risk of serious physical or personal safety, psychological, emotional, financial or reputation harm from the breach, but one of the following applies, the Manager or Nominated Officer is required to notify the Executive Director, Strategy and Governance:

- the breach has occurred on multiple occasions or with other breaches
- there is a risk of disclosure of organisationally sensitive information to third parties
- the breach indicates a systemic problem in QPT's processes or procedures
- the breach may result in financial loss to QPT
- the breach could result in a loss of public trust in QPT or the services it provides
- there is a threat to QPT's systems, which could, or is, impacting its capacity to provide services.

The Executive Director, Strategy and Governance will assess all information available and form a view as to whether the breach requires the activation of other response plans to ensure business continuity.

## 5. Consider notification to affected individuals and the Office of the Information Commissioner

The OIC strongly encourages all Queensland public agencies to notify affected individuals when a privacy data breach has occurred.

Where a breach is determined by the Executive Director, Strategy and Governance as having caused or poses a risk of serious harm to an affected individual, a notification to the OIC **must** be made.

Where a breach has not caused or poses a risk of serious harm, the Manager or Nominated Officer must consider and decide whether they will notify affected individuals. In general, if a breach creates a risk of harm

to an individual, the Manager or Nominated Officer should ensure the affected individuals are notified. The OIC recognises that there are occasions where notification can be counterproductive and cause stress or harm. For example, notifying individuals about a breach which is unlikely to result in an adverse outcome for the individual but may cause unnecessary anxiety and de-sensitise them to a significant privacy data breach.

When deciding whether to notify an individual that a breach has occurred, the Manager or Nominated Officer should consider:

- What is the risk of harm to the individual (as determined in Step 4)?
- Has QPT already taken sufficient steps to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual to take further steps to avoid or remedy harm?
- Are there regulatory or law enforcement reasons why individuals should not be notified (such as a criminal investigation)?

If the Manager or Nominated Officer decides the individual should be notified, this can occur over the phone, but must also occur in writing (either by email or post). The notification should describe what has happened including the date the breach occurred and/or was discovered, exactly what personal information was released, how the breach happened and any actions that have already been taken or are planned to prevent a similar breach occurring in the future, recommendations about the steps the individual should take in response to the breach, and the contact details of the Manager/Nominated Officer or a more senior officer within the organisational unit. Care must be taken to ensure the written notification does not inadvertently include personal information of any other customer or third party, including QPT staff member/s involved.

## 6. Review to prevent future breaches

Once the privacy data breach has been resolved and any affected individuals have been notified (if appropriate), the Manager or Nominated Officer must review all of the information gathered during the investigation to ensure the cause(s) of the breach are fully known and understood.

The Manager will then identify and implement any action(s) necessary to help prevent the same or similar breaches from occurring again in the future. If the investigation has been carried out by a Nominated Officer, they will report back to CSG who will provide advice to the Manager of the relevant organisational unit on actions or next steps.

The preventative actions required will depend on the type and cause of the breach, but some examples include:

- Providing additional training or guidance to staff members involved
- Updating internal manuals and practices
- Ensuring there is appropriate physical security in place
- Restricting access to certain systems, documents or files
- Suggesting changes to QPT policies or procedures
- Reviewing contractual obligations with contracted service providers
- Arranging for a security audit to be undertaken

- Other actions as per relevant QPT policies, such as those relating to fraud, corruption, employee performance management, information security, recordkeeping, etc.

The Manager must update CSG with information about the cause of the breach and any actions that are planned or have been taken. This information will then be recorded on QPT's internal Privacy Breach Register and may be shared with other entities if required or permitted under legislation.

## Annual Testing

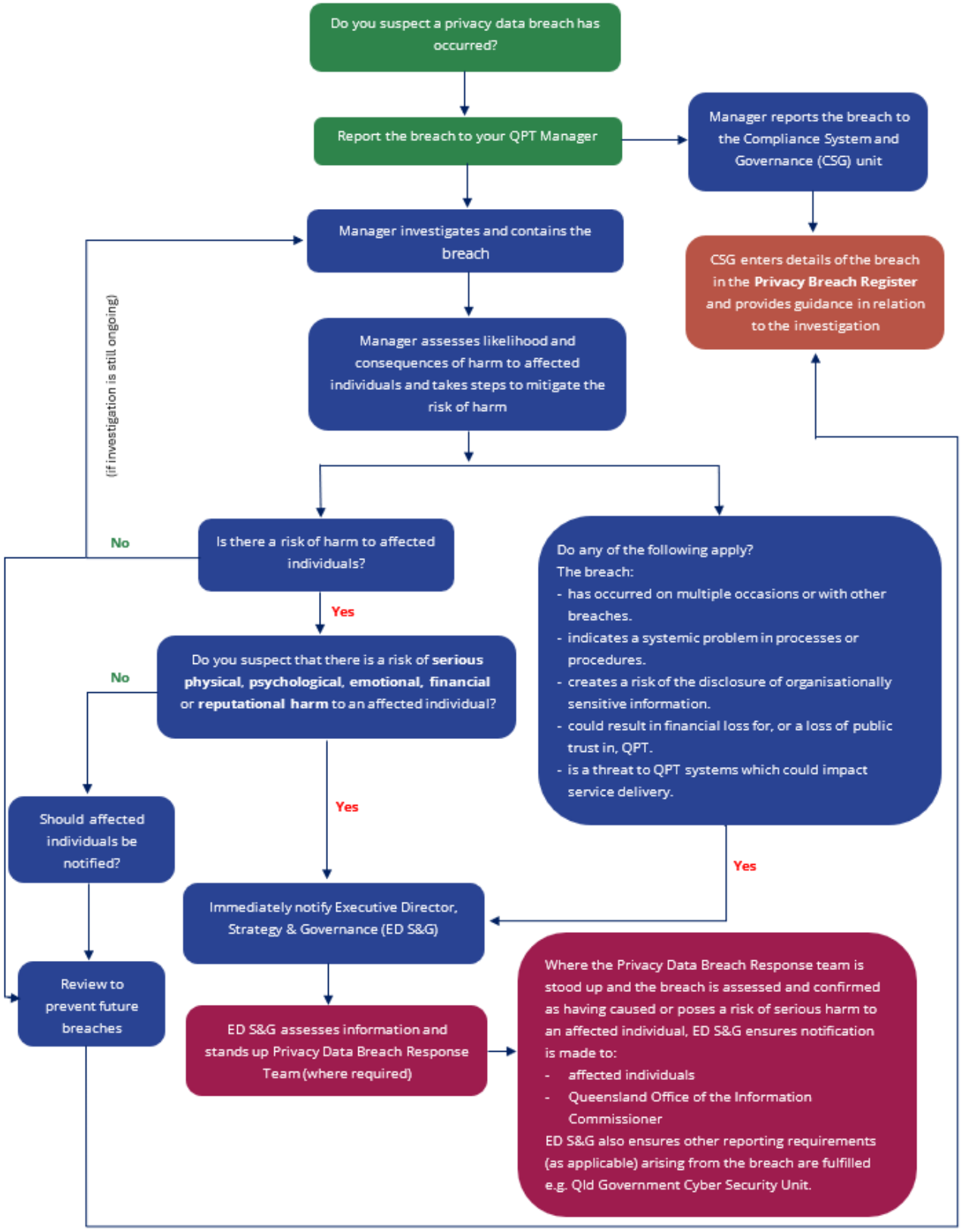
This Plan must be tested with the Executive Leadership Team (ELT) at least once every 12 months, using a hypothetical privacy data breach scenario to ensure its currency and utility.

The Director, CSG must report to the Reform and Management Group on the outcome of each annual test and any recommendations for improving this Plan.

## Related documents

Information Privacy Framework
Information Privacy Complaints Management Policy
Information Privacy Complaints Management Procedure
Information Privacy Statement
Right to Information Procedure
Business Continuity Plan
Crisis Management Plan
Information Technology Disaster Recovery Plan
Information Security Incident Management Standards
Fraud and Corruption Control Policy, Procedure and Plan
Queensland Office of the Information Commissioner – MNDB assessment tool

## APPENDIX A – Privacy Data Breach Response Flowchart



## APPENDIX B – Privacy Data Breach Response Team

When the Executive Director, Strategy and Governance is notified that there is a suspicion that a privacy data breach has occurred that may have caused or poses a risk of serious harm, they will consider all of the facts provided and decide whether the breach has caused or poses a risk of serious harm (refer to '4. Assess and mitigate risks' above for guidance).

Where this is the case, the Executive Director, Strategy and Governance will stand up a Privacy Data Breach Response Team to take over the handling of the breach from the Manager or Nominated Officer. The Executive Director, Strategy and Governance decides who needs to be included in the Response Team. This will typically include the roles shown in the table below.

The Privacy Data Breach Response Team is a temporary team that may only be established and led by the Executive Director, Strategy and Governance and is responsible for investigating and responding[4] to breaches that may have caused or pose a risk of serious harm that occurs within QPT, and incidents requiring reporting to the Australian Signals Directorate's Australian Cyber Security Centre, Queensland Government Cyber Security Unit, police/law enforcement, the Queensland Office of the Information Commissioner (OIC), or other body as required under law.

| Position | Responsibility and authority |
|---|---|
| Executive Director, Strategy and Governance<br><br>(Response Team Leader) | Decides if a breach has caused or poses a risk of serious harm and if a Privacy Data Breach Response Team is to be formed, including roles and key personnel.<br><br>Coordinates and authorises actions to investigate and respond to such breaches, including notifying the Queensland Government Insurance Fund (QGIF) or another insurer if relevant.<br><br>Ensures the Public Trustee of Queensland and CEO, and other members of Reform and Management Group are appropriately briefed.<br><br>In collaboration with members of the Response Team, determines if the breach or response to the breach is a 'crisis' – i.e. an abnormal or extraordinary event or situation that threatens QPT and requires a strategic, adaptive and timely response in order to preserve QPT's viability and integrity. (If so, the situation is to be managed in accordance with QPT's Crisis Management Plan). |
| Director, Compliance Systems and Governance | Supports the Response Team Leader to coordinate the response, including coordinating meetings of the Response Team, ensuring records are kept and a review is prepared after the breach has been resolved.<br><br>Acts as the conduit between organisational units involved in the breach and the response, including gathering information as needed to inform actions and response.<br><br>Coordinates engagement of internal or external experts if additional advice, including legal advice, is required. |

[4] Where notification of the breach is required to be made to OIC, the notification must in line with s 51 of the IP Act.

| Position | Responsibility and authority |
|---|---|
| Other staff within CSG | Support the Executive Director, Strategy and Governance and Director, Compliance Systems and Governance (as required).<br><br>Maintain records, including updating the Privacy Breach Register and ensuring all documents created by the Response Team, including post-breach evaluations and annual tests, are saved in Content Manager by CSG. |
| Chief Information Officer | Provides technical advice on any information technology related element to the response and directs, as line manager, any actions required of the Information and Technology unit. |
| Director, Strategic Engagement and Community Education<br><br>&<br><br>Director, Media | Develop a communication strategy, and coordinate, advise and prepare for approval any messages for widespread communication, including advice to customers, internal communications to staff and media statements/responses. |
| Executive Director and Director of organisational unit affected by the data breach or where the breach occurred. | On advice from the Response Team Leader, manages the local response including customer notifications (if appropriate),[5] mitigation and practice change – as line managers of the unit, authorised to direct actions of the staff within their organisational unit. |
| Other personnel as required | This may include internal or external experts, for example IT specialists, legal practitioners, risk management experts, HR personnel, etc. |

[5] Where the breach has caused or poses a risk of serious harm serious physical, psychological, emotional or financial harm, or serious harm to the individual's reputation, affected individuals must be notified in line with the specific notification requirements prescribed in s 53 (2) of the IP Act.