Data breach policy and response procedure

1. Purpose

This data breach policy and response procedure describes the processes for responding to a data breach or eligible data breach involving the unauthorised access to or unauthorised disclosure of, or the loss of, personal information (as defined under the *Information Privacy Act 2009* (IP Act)). It includes key considerations, actions and roles and responsibilities in the event of a data breach.

2. Scope

This policy and procedure applies to all:

- department employees as defined under the *Public Sector Act 2022* (the PS Act), except employees of the Office of Industrial Relations[1]
- labour hire contractors and trainees
- employees from another department or public sector entity on secondment or mobility arrangement under the PS Act

3. Definitions

Unless otherwise defined, the terms in this policy and procedure have the meaning as set out in IP Act.

Refer to **Appendix A** for definitions of key terms referred to in this policy and procedure.

4. Context

Data can be exposed to risk through cyber-attacks, system and process failures, human error, misconduct and loss or theft of computer hardware.

A 'data breach' occurs in relation to information held by an agency when there is:

a) unauthorised access to, or unauthorised disclosure of, the information; or

b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur[2].

If a data breach occurs, it must be assessed to determine whether the data breach is an 'eligible data breach'.

An 'eligible data breach' occurs when there is:

1. unauthorised access to, or unauthorised disclosure of, **personal information** held by the agency and the access or disclosure is likely to result in serious harm to an individual to whom the personal information relates; or
2. personal information held by an agency is lost in circumstances where the unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur and if it were to occur, it would be **likely to result in serious harm** to an individual to whom the personal information relates.

The department implements practices to minimise the risk of a data breach occurring including:

- the implementation of an Information Security Management System (ISMS),
- the application of security controls to the systems and information it holds,
- investment in cyber security capabilities to enable the detection and containment of data breaches, and
- testing the security measures and response processes it has in place.

All data breaches are evaluated individually by the Principal Information Officer, Privacy (Privacy Officer) to determine whether there has been any unauthorised access to, unauthorised disclosure or, or loss of, personal

[1] Employees of the Office of Industrial Relations (OIR) should refer to policy and procedural guidance of OIR.

[2] Schedule 5 of the IP Act

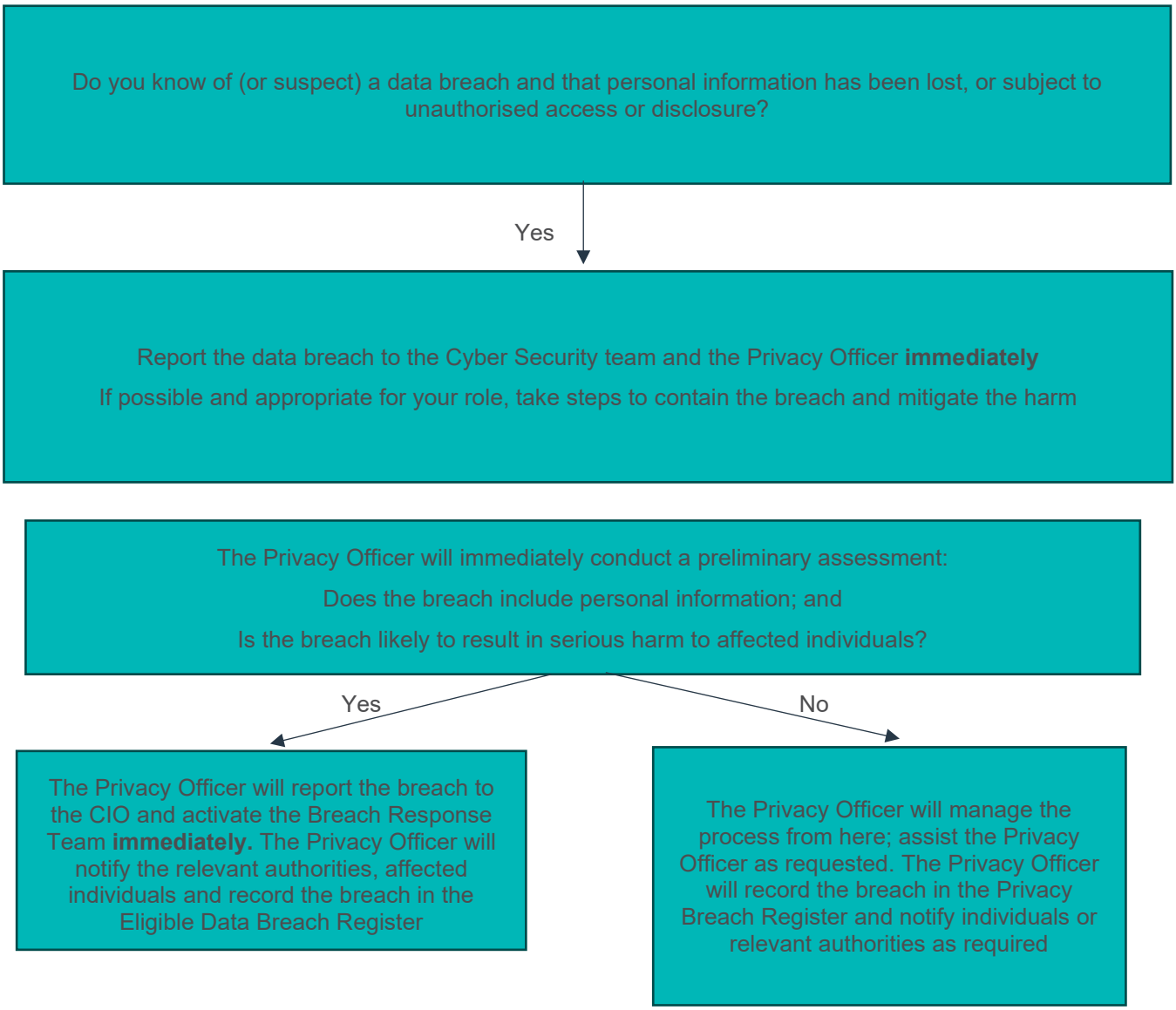
information. If a this has occurred, actions will be taken according to an assessment of risks and responsibilities based on the circumstances of the breach.

This policy and procedure are to be read in conjunction with the department's Privacy Policy (external link).

5. Procedure

5.1 Process overview

This policy and procedure set out the process to be followed where the department experiences a data breach or suspects that a data breach has occurred.



5.2 What should I do if I suspect a data breach has occurred?

It is everyone's responsibility to be aware of this policy and procedure and to report suspected data breaches as soon as possible.

In all cases, you must immediately report a suspected data breach by email to the Privacy Officer and to the Cyber Security team by email or via the ICT Service Desk.

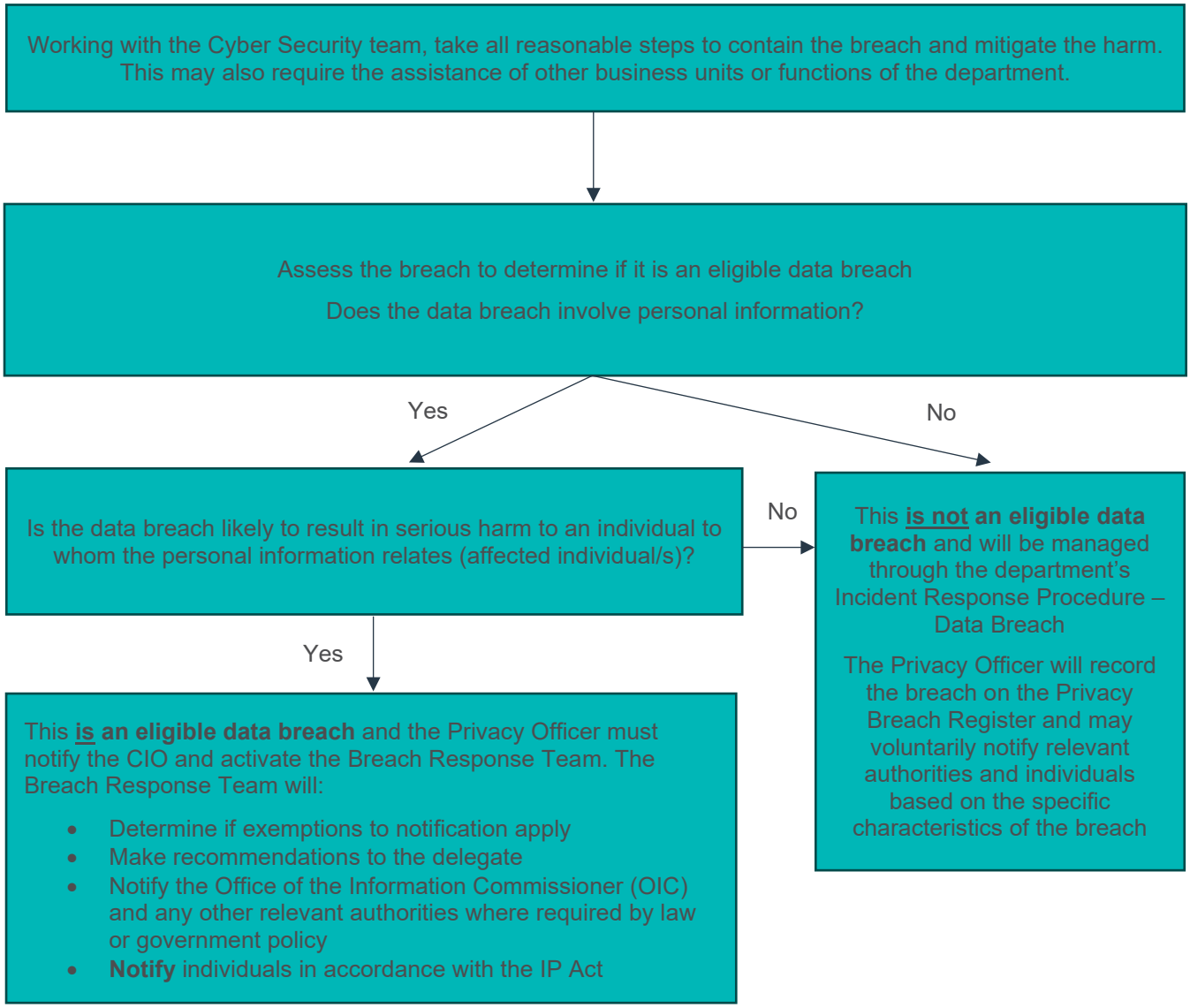
The Privacy Officer will immediately undertake a preliminary assessment to determine whether the breach does include personal information and if the breach is likely to cause serious harm to the affected individual/s. The Privacy Officer must log the breach in the department's Eligible Data Breach Register.

Depending on the nature of the data breach, it may be considered a 'notifiable data breach' under privacy law which requires the department to notify the Office of the Information Commissioner (OIC) and the affected individuals, with very few exceptions.

The Office of the Australian Information Commissioner (OAIC) must be notified where Tax File Numbers (TFNs) are included in the data breach. The Privacy Officer will make an assessment regarding the need to notify the OAIC in accordance with the process detailed below.

Even if a data breach has been contained, for example a misplaced laptop or hard copy files have been retrieved, the incident must be reported to the Privacy Officer. The Privacy Officer will assess any residual risk, and they can also consider whether further preventative action can be taken to avoid repeat occurrences.

5.3 Process overview for the Privacy Officer



5.4 Step 1: Contain the breach and mitigate the harm

- Once a data breach has been identified or reported, the department will immediately take all reasonable steps to contain the data breach and limit any further access or disclosure of the affected personal information.
- 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, revoking access by relevant system users, changing passwords and system usernames.
- Understanding how the data breach occurred will help in identifying the appropriate steps to contain it.
- The department will conduct preliminary fact-finding about the data breach.
- This will involve finding out the cause, risk of spread, and nature of the personal information involved in the data breach, options to mitigate, number and the location of the individuals affected.
- If the data breach involves a contracted service provider, the department will consider involving them as soon as possible.

5.5 Step 2: Assess whether the breach is an eligible data breach and document the risks to the affected individuals

- For monitoring purposes, the Privacy Officer will notify the Chief Information Officer (CIO) and Director, Information, ICT Governance and Spatial of the breach.
- The department will consider whether the data breach is likely to result in harm to any of the affected individuals. The department will continue to take all reasonable steps to prevent or lessen the likelihood that the data breach will result in harm to any individual.
- This step may take place at the same time as the data breach is being contained and assessed. Remedial action will depend on the nature of the data breach but may involve recovering lost information before it is accessed or changing access controls on system accounts before access to, or unauthorised transactions can occur.
- The department will complete an assessment of the harm that may eventuate from the data breach.
- The assessment must determine whether there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in, serious harm to one or more of the individuals to whom the information relates. This includes considerations of:
  - the type/s of personal information
  - the sensitivity of the information
  - whether the information is protected by one or more security measures
  - the likelihood that the security measures could be overcome
  - the person (or kind of person/s) who have obtained, or could obtain, the personal information
  - the nature of the harm likely to result from the data breach
  - other relevant matters. This might include how long the information was exposed, the circumstances of the affected individual, how the breach occurred, to what extent has the harm or risk of harm been minimised by the mitigation action taken by the department.
- This assessment must be completed immediately. Where the agency does not know whether the data breach is an eligible data breach, the agency will assess whether there are reasonable grounds to believe the data breach is an eligible data breach within 30 calendar days. The assessment must be documented.
- For eligible data breaches, the Breach Response Team will consider whether to involve any other internal or external parties at this stage, for example:
  - If the data breach involves multiple agencies, the department will liaise with the other agency / agencies to determine who will be responsible for assessing the data breach within the required period, and whether a joint response team should be formed.
  - For other types of criminal activity (e.g. theft), the department will contact the local police.

5.6 Review containment steps and remediate further if required

- An assessment of the steps taken to date will be undertaken. It is possible that more information is known about the extent of the breach and information involved at this stage. Any further steps to contain the breach and mitigate harm will be implemented.
- For eligible data breaches, if there is a risk that the personal information could be used for identity theft or other types of fraud, the department may engage with IDCARE, the National Identity & Cyber Support Service, on 1800 595 170, or via www.idcare.org. IDCARE can offer the department advice and can also assist affected individuals.

5.7 Step 3: Notify and communicate

- Unless an exemption applies, an agency is required to notify the OIC of an eligible data breach.
- Notification to the OAIC is required by law under the Commonwealth *Privacy Act 1988* (Cth) (Privacy Act (Cth)) if Tax File Numbers (TFNs) were involved and the assessment has concluded there are reasonable grounds to believe the data breach has resulted in or is likely to result in serious harm to one or more of the individuals to whom the information relates (i.e. what we describe as a High Risk breach).
- Notification to individuals and the OIC is voluntary in all other cases.
- Where an eligible data breach occurs, there are three options for notifying individuals:
  a) Directly notifying all individuals whose personal information was accessed, disclosed or lost in the eligible data breach, or if that is not reasonably practicable;
  b) Directly notify only those individuals at risk of serious harm, or if that is not reasonably practicable;
  c) Publish the statement on an accessible agency website for at least 12 months.
- The department must notify individuals in this way unless a statutory exemption applies, such as:
  - if notification would prejudice an investigation or court proceedings,
  - breach a secrecy provision,
  - create a serious risk of harm to an individual's health or safety, or
  - if notification would compromise or worsen the agency's cyber security, or lead to further data breaches.
- Where it is not reasonably practicable to identify and directly notify individuals whose personal information has been accessed, disclosed or lost, then the department will take reasonable steps to directly notify all individuals who are likely to suffer serious harm.
- Where it is not reasonably practicable to take these steps, then a notification will be published on the department's website for at least 12 months. The department will take reasonable steps to publicise that notification and consider additional methods of communication such as social media, or advertisements in newspapers, as appropriate.
- Where appropriate, social media may be used to provide information about the investigation, any updates and what further action individuals may take and what steps the department is taking to prevent any future data breaches.
- As soon as practicable, the department will prepare and provide to the OIC, a statement which provides information about the eligible data breach.
- In relation to a data breach involving TFNs, a statement will be sent to the Australian Privacy Commissioner (part of the OAIC) in accordance with the requirements of relevant federal legislation.
- Where an eligible data breach affected more than one agency, notification to the OIC and relevant individuals may be made by the agency that undertook the assessment of the data breach.
- If the data breach involves a contracted service provider, the contracted service provider may be required to cooperate with the department and a position will be determined on a case-by-case basis.
- Depending on the number of individuals affected, a dedicated webpage, and/or telephone line may be set up.
- The department will consider whether any other entities, such as regulatory bodies, financial institutions, insurance companies or credit reporting agencies should also be notified.

5.8 Step 4: Prevent future breaches

- Impacted business unit's procedures and systems will be reviewed and updated to mitigate the occurrence of similar recurrent breaches.
- Training and awareness will be provided to the impacted business unit where appropriate.
- Eligible data breaches will be added to the department's internal Eligible Data Breach Register.[3]
- Mitigation steps will address the identified root cause of the data breach. Mitigation may include: a security audit and any modifications to physical controls such as locks, alarms, visitor access control, review of policies and procedures including the privacy management framework, review of employee training and selection practices, a review of suppliers and third parties, updating passwords, or altered deployments of technology.
- For eligible data breaches, a review of the response process will be conducted after the process concludes with details of any recommendations recorded and improvements implemented in a timely manner.
- The Privacy Officer will ensure all data breaches are recorded in the Eligible Data Breach Register, and instruct business units to maintain appropriate records, to provide evidence of how suspected data breaches are managed. Tracking data breaches allows the department to monitor, analyse and review the type and severity of suspected and actual data breaches.
- The Privacy Officer will conduct an annual review of the department's breach response records, to identify opportunities to enhance departmental practices.

6. Breach Response Team

The Breach Response Team will be comprised of the following roles. Additional roles may be recruited depending on the characteristics of the breach:

- Chief Information Officer
- Director, Information, ICT Governance and Spatial
- Manager, Cyber Security
- Director, Strategic Communications
- Executive Director of the affected business unit/s
- Director, Human Resources
- Director, Integrity and Workplace Relations
- General Counsel or Director, Legal Services.

7. Human rights compatibility

The department is committed to respecting, protecting and promoting human rights.

Under the *Human Rights Act 2019* (HR Act), all public entities (including the department and its employees) have an obligation to act and make decisions in a way that is compatible with human rights and, when making a decision, to give proper consideration to human rights.

When acting or making a decision under this procedure, decision-makers must comply with this obligation.

8. Responsibilities

Role	Responsibilities
Delegates	• Exercise delegated functions or powers in accordance with the department's delegations, all relevant statutory provisions, whole-of-government policy and directives and principles of procedural fairness.
Director-General (DG) (accountable officer)	• Set the ethical culture of the department including a commitment to information privacy and compliance with the Information Privacy Act 2009 and mandatory notification of data breach (MNDB) requirements.

[3] Section 72 of the IP Act.

Role	Responsibilities
Employees	• Maintain awareness of information privacy requirements • Comply with the Privacy Policy and this Data Breach Policy & Procedure.
All business units	• Cooperate with the Privacy Officer and Breach Response Team if requested to provide information or assistance in responding to a data breach.
Managers and supervisors	• Ensure employees under their supervision are aware of the requirements of this Data Breach Policy & Procedure.
Privacy Officer	• Perform the actions referenced in this Data Breach Policy and Response Procedure & maintain appropriate records in relation to data breaches.
Breach Response Team	• Manage the response to an eligible data breach in accordance with this policy and procedure and communicate and escalate activities as required.

9. Related documents, forms and templates

- Privacy Policy (external link)

10. References

- Code of Conduct for the Queensland Public Service
- *Human Rights Act 2019*
- *Industrial Relations Act 2016*
- *Information Privacy Act 2009*
- *Public Records Act 2023*
- *Public Sector Act 2022*
- *Right to Information Act 2009*
- Privacy principles guideline - Assessing a Data Breach (Office of the Information Commissioner)

11. Further information

For further information or clarification, please contact privacy@dsdilgp.qld.gov.au.

12. Storage of information

All information should be managed in accordance with the *Public Records Act 2023*, and the whole-of-Government Records Governance policy**.** In addition, personal information should be managed in accordance with the *Information Privacy Act 2009*.

13. Document control

Policy owner		Executive Director and Chief Information Officer, Information and Technology Services (ITS), Corporate		
Contact details		privacy@dsdilgp.qld.gov.au		
Next review		June 2027		
Supersedes		N/A (new document)		
Version	**Issue Date**	**Reason**	**Author**	**Approver**
1.0	30/06/2025	New document	Principal Information Officer (Privacy), ITS	Deputy Director-General, Corporate

Appendix A: Definitions

The key terms referred to in this policy and procedure are as follows:

Term	Definition
Delegate	• The person authorised to perform a specific task or function under legislation on the Director-General or Minister's behalf. Delegations are recorded in the department's delegation schedules.
Personal information	• Personal information means information of an opinion about an identified 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. (Section 12 of the IP Act)
Serious harm	• Includes serious physical, psychological, emotional, financial or reputational harm.