Data breach policy

Reference number	PRI.003
Document owner	Manager, Privacy and Right to Information
Contact details	rtiandip@desbt.qld.gov.au
Effective date	1 July 2025
Next review	1 July 2027

1. Purpose

The purpose of this document is to outline how the department will respond to a data breach, or suspected data breach, of the department, in accordance with section 73 of the *Information Privacy Act 2009* (Qld) (IP Act).

2. Scope

This policy applies to all employees working for the department regardless of whether they are permanent, temporary, full-time, part-time or casual employees and/or on secondment from another department. It also applies to non-employees including contractors, students gaining work experience and volunteers. For the purposes of this policy, the term contractor includes temporary labour services (agency staff).

3. Key definitions

'*Data breach'*, of an agency, means either of the following in relation to information held by the agency –

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

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

An '*eligible data breach'* of an agency is a data breach of the agency that occurs in relation to personal information that is likely to cause serious harm to the individual to whom the personal information relates.

'*Personal information'* means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion. It includes, names, dates of birth, contact information, signatures, and qualifications.

The likelihood of serious harm is to be determined having regard to –

a) the kind of personal information access, disclosed, or lost
b) the sensitivity of the personal information
c) whether the personal information is protected by 1 or more security measures
d) if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome
e) the persons, or kinds of persons, who have obtained, or who could obtain, the personal information
f) the nature of the harm likely to result from the data breach
g) any other relevant matter

4. Contain

If any employee knows, or reasonably suspects, that a data breach has occurred, they must immediately notify their manager or director and the Privacy Officer in writing.

If the employee, manager, or director knows, or reasonably suspects, that the data breach involves personal information of an individual and may cause serious harm to the individual, they must immediately make the Privacy Officer aware of this.

The employee, manager, and director should take all practicable steps to contain the data breach by, for example:

- If the breach occurs as a result of an email sent to an incorrect email address, asking the recipient to confirm that they have permanently deleted the email
- If the breach occurs as a result of an employee mistakenly accessing a document they should not be able to access, advising in writing that the employee has closed the document and is no longer accessing it
- If the breach occurs as a result of an employee leaving documents in a public setting and it is practicable to do so, returning to the place the documents were last seen
- If the breach occurs as a result of a party gaining remote access to electronic systems, seeking advice from ICT and following that advice.

If the employee, manager, or director require any advice or suggestions about steps they can take to contain the breach, they should consult with the Privacy Officer.

The manager and director should report the occurrence to their Executive Director.

All steps taken to contain the breach should be documented.

5. Mitigate

The department has ongoing obligations to mitigate any harms caused by the breach after it is contained.

If the breach is likely to cause an immediate risk to a person's law, health or safety, the employee must call 000 immediately.

If the breach is likely to cause imminent, irreparable physical, psychological or financial harm, the employee must consider immediate action or notification. Once that action is taken, the employee should notify their manager and director as soon as practicable, who should escalate the issue to the attention of the relevant Deputy Director-General and Director-General.

If the breach is likely to cause serious harm but those harms are unlikely to occur immediately, the employee should discuss with their manager, director and the Privacy Officer in the first instance.

That group is responsible for identifying what harms are likely to occur, who is best placed to mitigate those harms (whether the affected individual or a member of the department), and what actions might be taken to mitigate the harm.

6. Assess

The Privacy Officer must, within 30 business days (approximately six weeks) of the day that an employee first suspected the data breach, assess whether the data breach is an eligible data breach.

If the Privacy Officer determines that the breach is not an eligible data breach, the Privacy Officer is to record the reasons for concluding this in writing and notify the employee, manager and director.

If the Privacy Officer determines that the breach is an eligible data breach and that there is a relevant exemption to the notification requirements, the Privacy Officer will record this in writing.

7. Notification

If the Privacy Officer determines that the breach is an eligible data breach and no exemption applies, they must notify the Information Commissioner and provide all of the necessary details in section 51(2) of the IP Act.

If it is not reasonably practicable to provide all of the relevant details, the Privacy Officer will request further information from the director of the relevant unit, so that those details can be subsequently provided to the Information Commissioner.

If the breach is an eligible data breach, the Privacy Officer is responsible for drafting a letter to the affected individual/s containing the relevant information in section 53(2) of the IP Act.

8. Post incident review

The Privacy Officer is responsible for including the relevant details in the Eligible Data Breach Register.

The director of the relevant unit is responsible for assessing the likelihood that a similar breach may occur in future and the impact of the breach.

Alternatively, the director of the relevant unit may decide to change a relevant personal information handling practice, with a view to preventing a recurrence. A Privacy Impact Assessment should be conducted in accordance with the Privacy Impact Assessment Procedure.

9. Other agency involvement

If the employee who first know, or reasonably suspects, that a data breach has occurred, is aware that the breach may affect another government agency, they should notify the Privacy Officer.

The Privacy Officer may provide the second agency with a description of the data breach and a description of the personal information involved in the breach, so that agency may also take appropriate remedial action.

10. Responsibilities

Role	Responsibilities
Director-General	• Ensure all employees abide by this policy
Executive Director	• Oversee suspected data breaches and report to Deputy Director-General as appropriate
Manager/Director	• Ensure that all data breaches are reported to the privacy officer and that all reasonable steps to contain and mitigate the breach are undertaken • Consider whether a Privacy Impact Assessment is required • Report suspected data breaches to the Executive Director

Employees	• Report all data breaches to their manager or supervisor as soon as practicable • Take all reasonable steps to contain the breach as soon as practicable
Privacy Officer	• Provide advice on options to contain or mitigate privacy breaches • Assess whether the breach involves personal information and or a risk of serious harm to an affected individual • Comply with the statutory notification and reporting requirements of eligible data breaches • Maintain the eligible data breach register • Take feedback back to the business area

11. Human Rights Capability

The department is committed to respecting, protecting and promoting human rights. Under the *Human Rights Act 2019*, the department has 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 making a decision relating to privacy, decision-makers must comply with this obligation.

Most relevantly, the department must ensure it does not unlawfully or arbitrarily interfere with your privacy or that, if it does so, it does so in a way that is reasonable and justifiable. This procedure is designed to ensure that the department will act and make decisions in accordance with the *Information Privacy Act 2009* (Qld) and as consistently across the department as practicable. To the extent that the procedure limits the right to privacy, it does so consistently with applicable legislation and the practical requirements of administering that legislation.

For further information on human rights, see:

- QHRC: Queensland Human Rights Commission
- Human rights | For government | Queensland Government

12. References

- *Information Privacy Act 2009 (Qld)*
- *Human Rights Act 2019 (Qld)*
- *Right to Information Act 2009 (Qld)*
- *Public Sector Act 2022 (Qld)*
- *Public Records Act 2023 (Qld)*
- Queensland Government information security classification framework
- Queensland Government general retention and disposal schedule

13. Further information

For further information or clarification, please contact the Manager, Privacy and Right to Information.

14. Document control

Review frequency			Biennial			
Supersedes			N/A			
Version	Issue date	Reason	Author	Approver	Date of Approval	Ref
1.0	01/07/2025	Initial release	Manager, Privacy and Right to Information	Director-General		