Economic Development Queensland (EDQ)

Data Breach Policy

Version: 1.0 | Version effective: 4 February 2026

1. Policy statement

Economic Development Queensland (EDQ) is committed to protecting personal information in accordance with the *Information Privacy Act 2009* (IP Act). This policy establishes the framework needed to properly identify, assess and respond to any data breach or suspected data breach involving the unauthorised access, unauthorised disclosure or loss of personal information. It establishes the responsibilities and actions required to ensure that any data breach is promptly identified, assessed and managed to minimise harm. This policy is to be read in conjunction with the Privacy Policy and the Data Breach Response Plan.

2. Rationale

EDQ recognise that a formal Data Breach Policy is necessary to meet obligations under the IP Act and to ensure a consistent, lawful and accountable approach to managing data breaches.

The Mandatory Notification of Data Breach (MNDB) scheme requirements apply to service providers in circumstances where data breaches involve personal information that is in the possession of a contracted service provider (CSP). When a data breach occurs which involves information in the possession of a CSP, EDQ will carefully examine whether the information is considered to be 'held' by EDQ, by considering all relevant circumstances, such as EDQ's relationship with the information and relevant legislation and guidelines.

3. Applicability

This policy applies to all employees and temporary and contracted workers of EDQ, and Economic Development Board (Board) members.

4. Principles

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 (Schedule 5 of the IP Act).

If a data breach occurs, the Privacy Officer is notified, and it must be assessed to determine whether the data breach is an 'eligible data breach'. An 'eligible data breach' occurs when there is:

a) unauthorised access to, or unauthorised disclosure of, **personal information** held by EDQ and the access or disclosure is likely to result in serious harm to an individual to whom the personal information relates; or

b) personal information held by EDQ 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.

EDQ 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
- testing the security measures and response processes it has in place.

All data breaches are evaluated individually by the Privacy Officer to determine whether there has been any unauthorised access to, unauthorised disclosure or, or loss of, personal information. If this has occurred, actions will be taken according to an assessment of risks and responsibilities based on the circumstances of the breach.

5. Roles and responsibilities

Role	Responsibilities
All employees	• Notify the Privacy Officer of any data breach or potential data breach. • Comply with this policy, the Privacy Policy and all relevant legislative obligations. • Protect personal information from unauthorised access, loss or disclosure by using approved systems and practices. • Participate in required training and maintain awareness of data breach requirements.
Audit, Risk and Performance Committee (ARPC)	• Reviews EDQ compliance with data breach requirements. • Provides recommendations to the Board on the effectiveness of EDQ privacy framework.
Board	• Approves the EDQ Data Breach Policy. • Notify the Privacy Officer of any data breach or potential data breach.
Chief Executive Officer	• Set the ethical culture of EDQ including a commitment to information privacy, compliance with the IP Act and mandatory notification of data breach requirements.
Data Breach team	• Manage the response to an eligible data breach in accordance with this policy and response plan and communicate and escalate activities as required.
Managers and supervisors	• Ensure employees under their supervision are aware of the requirements of this policy.
Privacy Officer	• Provide advice and guidance relating to the application of this policy and requirements of the IP Act.

6. Definitions

The key terms referred to are as follows:

Term	Definition
Board	The Economic Development Board as defined in the ED Act (Schedule 1 – Dictionary).
Chief Executive Officer	The Chief Executive Officer (CEO) as defined in the ED Act (Section 32Q (1)).
Contracted service provider	A contracted service provider (CSP) is any external organisation or individual engaged by EDQ to deliver services on their behalf, where the provider has possession of, access to, or responsibility for handling personal information while performing those services.
Data Breach team	A data breach team is a group of designated roles within EDQ responsible for coordinating the response to an actual or suspected data breach, including assessing impacts, managing containment actions, and ensuring compliance with legislative and policy requirements.
ED Act	*Economic Development Act 2012* (ED Act).
EDQ	MEDQ and the EDQ Employing Office
EDQ Employing Office	The Economic Development Queensland employing office is a statutory body as defined in the ED Act (Part 9, Division 1).
Employee	Includes the CEO (Section 32Q (1)), EO (Section 32ZK) and EDQ employees (Schedule 1 – Dictionary) as defined in the ED Act and contractors.

Term	Definition
IP Act	*Information Privacy Act 2009.*
MEDQ	A corporation sole constituted by the Minister established under the name Minister for Economic Development Queensland as defined in the ED Act (Section 8 (1)).
Personal information	Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion (per IP Act, section 12).
Serious harm	Includes serious physical, psychological, emotional, financial or reputational harm.

7. References

Legislation / subordinate legislation

- *Economic Development Act 2012*
- *Human Rights Act 2019*
- *Industrial Relations Act 2016*
- *Information Privacy Act 2009*
- *Public Records Act 2023*
- *Public Sector Act 1994*
- *Public Sector Ethics Act 1994*
- *Right to Information Act 2009*

Other documents or processes

- Code of Conduct for the Queensland Public Service
- Crisis Management Policy
- Data Breach Response Plan
- Privacy Policy

8. Policy approval

This policy will be reviewed by the Board biennially. All major policy changes must be approved by the Board. The Director, Governance is authorised to approve minor policy amendments. Minor policy amendments are those that do not change the overall intent of the policy. A register of amendments will be maintained and reported annually to the Board.

9. Document control

Document owner		**Director, Governance Corporate Services**			
Major review (biennially)		February 2028			
Version	**Issue Date**	**Reason**	**Author**	**Approver**	**Approval date**
1.0	Feb 2026	New policy	Director, Governance	Board	4/02/2026