Policy

I22 Security incident, event, and data breach management

Purpose

This policy defines our combined approach for responding to security incidents, events, and data breaches, including eligible data breaches, to ensure we comply with all relevant statutory legislation and fulfil our mandatory reporting obligations.

This policy should be taken as QAO's Data Breach Policy.

Application

This policy applies to the QAO workforce. This includes permanent, temporary, and contracted employees, as well as contractors and consultants.

It also applies to incidents or breaches reported to QAO by an audit service provider.

Legislative context

- *Auditor-General Act 2009*
- *Information Privacy Act 2009*
- *Privacy Act 1988* (Cth)
- Information and cyber security policy (IS18)

Definitions/glossary of terms

Term	Definition
Audit service provider	Audit firms who have been engaged to conduct audit work on behalf of the Auditor-General.
Cyber	Relating to or characteristic to the realm of information technology, technology hardware, software, information assets and the networks that link them
Data breach	An incident or series of incidents which results in sensitive information or data being compromised or lost, or subject to unauthorised use or disclosure.
Eligible data breach	Has the meaning given in s.33 of the *Information Privacy and Other Legislation Amendment Act 2023*. (Note: This will be section 47 of the amended *Information Privacy Act 2009*).
Privacy breach	A privacy breach occurs when personal information, as defined in s.12 of the *Information Privacy Act 2009,* is compromised or lost, or subject to unauthorised use or disclosure.
Security event	An identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant.
Security incident	A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. All incidents are events, but not all events are incidents.
Threat	A combination of capability (e.g., hacking skills), opportunity (e.g., system vulnerabilities) and intent (e.g., disgruntled ex-staff member).

Term	Definition
Threat actor	A person or group of persons partially or wholly responsible for an incident that impacts or has the potential to impact the organisation. Threat actors can be internal, external or partner

Policy statement

QAO will:

- identify, contain, investigate and report all known or suspected security incidents, events or data breaches including eligible data breaches
- comply with all mandatory reporting requirements e.g., eligible data breaches under the *Information Privacy Act 2009* (IP Act)
- conduct post-incident review activities to identify opportunities for improvement and/ or professional development to mitigate the risk of incidents or data breaches reoccurring
- develop and deliver privacy, security and incident response training to the QAO workforce
- maintain a security incident, event and data breach register
- make and keep records in accordance with the *Public Records Act 2023*.

Principles

Identify and contain

All known or suspected data breaches can be reported to QAO using the following details:

Email: qao@qao.qld.gov.au

Phone: 07 3149 6000

Similarly, if any unusual activity is detected in our environment then we will take immediate action to investigate, contain and respond to the security incident or event.

Audit Service Providers

Our audit service providers have an obligation to notify the Auditor-General of all security incidents or data breaches as soon as practicable.

Investigate

We will conduct a preliminary assessment of all data breaches and severe security incidents. Where possible, we will:

- summarise the details of the breach
- identify the affected parties
- identify the business impact level (BIL)
- describe any remedial action taken
- identify whether any external parties need to be engaged
- identify any external reporting requirements
- determine a course of action.

We will use a consequence and likelihood matrix to inform our decisions and response activities e.g., internal or external investigation, external reporting requirements, etc.

In the event of an eligible data breach, we will conduct a full investigation. This may include, but is not limited to interviewing relevant stakeholders, collecting evidence from affected parties, consulting with security specialists or obtaining legal advice. Once complete, an investigation report will be prepared to summarise the incident, key findings and actions to be taken.

Notify and report

As part of our assessment, we will determine whether the incident or event needs to be reported to an external party. This may include but is not limited to the following:

Regulatory authority	Description of circumstance
Office of the Information Commissioner (OIC)	Disclosure is required if the incident is an eligible data breach under the IP Act. Other privacy breaches can be voluntarily reported.
Office of the Australian Information Commissioner (OAIC)	Disclosure is required if the data breach is likely to result in serious harm to an individual where specific types of personal information are involved.
Australian Digital Health Agency	Disclosure is required if the incident results in any health data (as defined in section 75(1) of the *My Health Records Act 2012*) being compromised.
Cyber Defence Centre (CDC)	Disclosure may be required in the event of a security incident.
Queensland State Archivist	Disclosure may be required if the incident results in the loss or unauthorised destruction of a public record.
Queensland Police Service (QPS)	Disclosure may be required if the incident appears to involve theft or other criminal activity.
Crime and Corruption Commission (CCC)	Disclosure may be required if the incident involves corrupt conduct per the *Crime and Corruption Act 2001*.
Queensland Government Insurance Fund (QGIF)	Disclosure is required if we are affected by a cyber incident that results in a loss for QAO.

Crisis communication plan

We will maintain a crisis communication plan to help manage communications during crises. This may include data breaches and cyber security attacks.

The decision to activate our crisis plan could be made during the preliminary assessment or at any stage during the investigation. This decision will be made by the Auditor-General or Executive Leadership Team.

Review and mitigate

Once contained, we will reflect on the situation and make recommendations for ways to prevent future incidents or data breaches from occurring. This may include identifying business improvement opportunities or performing a root cause analysis. The key findings and recommendations will be presented to the Auditor-General.

Responsibilities

Role	Responsibilities
Auditor-General or delegate	• Ensure the QAO complies with relevant legislation and policies regarding data breaches.
Chief Information and Technology Officer	• Lead the technical response to data breaches, including containment, mitigation, and remediation. • Maintain the Register of Eligible Data Breaches. • Approve and oversee the implementation of post-breach remediation actions.
Data Breach Response Team	• Review, assess and remediate incidents escalated to the team. • Follow this policy when responding to a data breach.

Role	Responsibilities
	• Consult with internal and external stakeholders as require. • Determine if a Data Breach is an Eligible Data Breach.
Employees and contractors	• Report suspected or actual data breaches immediately. • Follow QAO policies and procedures to prevent data breaches • Respond to requests for information from and cooperate with the Data Breach Response Team. • Comply with recordkeeping obligations.
Audit Service Providers	• Notify the QAO promptly of any data breaches involving QAO work. • Comply with contractual obligations regarding data protection and breach notification.

Last approved: 12 August 2025