Industrial Registry
Mandatory Notification of Data Breach Policy and Response Plan

Version 1.1| **Date Effective:** 19 November 2025

1. Purpose and Scope

The Industrial Court of Queensland (Court), the Queensland Industrial Relations Commission (Commission) and the Industrial Registry are committed to the proactive management of **personal information** in accordance with the *Information Privacy Act 2009* (IP Act).

This policy outlines our commitment to protecting personal information in accordance with the IP Act, and sets out procedures for responding to both **data breaches** and **eligible data breaches**, including notification and mitigation steps, as required under the **mandatory data breach notification scheme**.

Where an eligible data breach is suspected or confirmed, the Industrial Registry will work with the **Office of Industrial Relations Privacy Team** (Privacy Team) to assess the breach, mitigate its effects, and ensure affected individuals are notified accordingly, as well as the **Office of the Information Commissioner** (OIC) or the **Office of the Australian Information Commissioner** (OAIC) where appropriate, in accordance with legislative requirements.

This policy applies to all staff, contractors and any third parties handling personal information on behalf of the Industrial Registry and is to be read in conjunction with the:

- Industrial Registry Privacy Policy;
- Office of Industrial Relations Privacy Policy; and
- Office of Industrial Relations Privacy Breach Response Procedure.

2. What is a data breach/Eligible Data Breach?

Data may be compromised through cyberattacks, ransomware, phishing, malware, system or process failures, social engineering, human error, deliberate misconduct, lost and stolen devices.

A data breach is defined in the IP Act to mean the unauthorised access or disclosure of information held by an agency or the loss of personal or non-personal information held by an agency where unauthorised access or disclosure is likely to occur.

However not all data breaches are an eligible data breach. An eligible data breach, as outlined in s 47 of the IP Act, is considered serious and always relates to an actual or potential loss of, unauthorised access to, or unauthorised disclosure of, personal information, which is "likely to result in serious harm" to one or more persons, and therefore is deemed a **mandatory notifiable data breach**.

3. Roles and responsibilities

It is the responsibility of all staff to:

- be aware of the Industrial Registry Privacy Policy and this Mandatory Notification of Data Breach and Response Plan, along with OIR's Privacy Breach Response Procedure (Procedure);

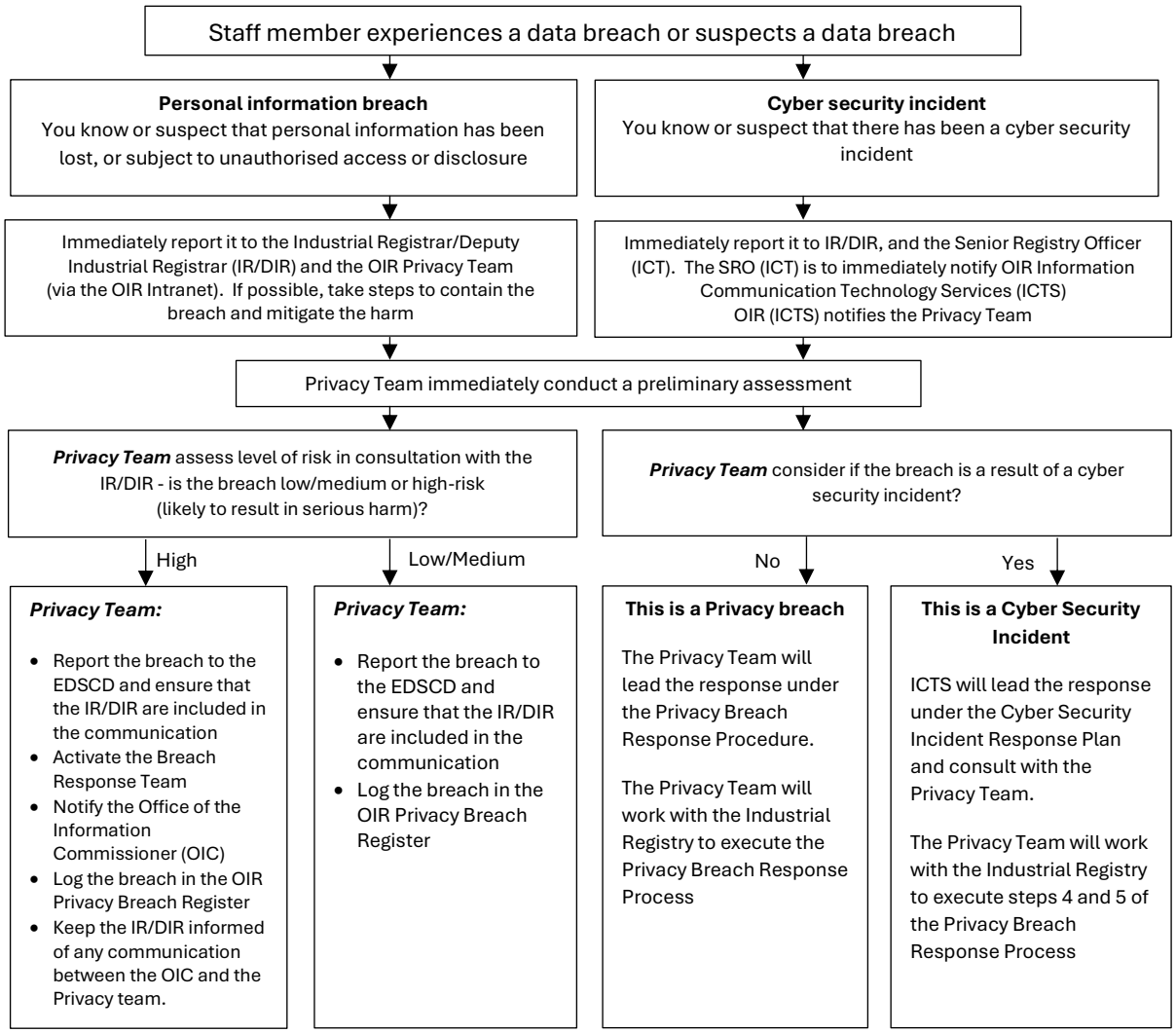
- comply with the IP Act, include protecting personal information held by the Industrial Registry from unauthorised access, disclosure or loss;
- immediately report a data breach or suspected data breach, to the Industrial Registrar/Deputy Industrial Registrar and the Privacy Team via the reporting system on the OIR Intranet;
- respond to, and cooperate with, requests for information from the Industrial Registrar and/or the Privacy Team; and
- comply with record keeping obligations.

It is the responsibility of OIR's Privacy Team, in consultation with the Industrial Registrar/Deputy Industrial Registrar, to:

- contain the breach;
- assess the breach and document the risks;
- in the case of a high-risk breach (e.g. cyberattack), escalate the incident to the **Executive Director Strategic Communications and Data** (EDSCD);
- review containment steps and remediate further if required;
- notify relevant parties and communicate to staff and stakeholders;
- take steps to prevent future breaches, in consultation with the Industrial Registrar.

4. Data breach/suspected data breach procedural overview

The following outlines the steps to follow in the event of a data breach or suspected data breach:



5. Response Plan

5.1 *Stage 1: Preparation*

The Industrial Registry will consult with the Privacy Team to ensure all foundational processes, policies and procedures are in place, are monitored and are reviewed annually.

5.2 *Stage 2: Identification and Reporting*

In the event of the identification of a suspected data breach, a staff member should immediately advise their manager or the Industrial Registrar/Deputy Industrial Registrar.

Should a staff member not be sure whether a suspected breach constitutes a data breach, they should consult with their manager or the Industrial Registrar/Deputy Industrial Registrar immediately.

Examples of a less serious ***data breach*** include:

- sending a generic email to the wrong recipient;
- accidentally accessing a secure database;
- leaving an encrypted USB or a security locked computer on public transport; or
- accidentally disclosing contact details to a government department, agency or entity.

Examples of a serious ***eligible data breach*** include:

- a staff member accidentally losing or misplacing documents containing sensitive or personal information, such as a Court or Commission file;
- a contractor disclosing sensitive or personal information to an external party;
- inappropriate access by a staff member or individual to a restricted internal file containing sensitive or personal information; or
- a cyberattack, phishing, malware or hacking incident.

Once identified as a data breach/eligible data breach, the Privacy Team are notified via the OIR Intranet reporting system.

All privacy breaches reported to the Privacy Team will be recorded in the **OIR Privacy Breach Register** (Register). The Industrial Registrar/Deputy Industrial Registrar will also maintain an internal register for recording purposes.

In the case of a notifiable data breach, the Privacy Team will notify the OIC and the affected individual/s, ensuring that the Industrial Registrar/Deputy Industrial Registrar are included in that communication.

If a Tax File Number (TFN) is included in the privacy breach, OAIC will be notified by the Privacy Team, once assessments have been conducted.

It is important that the Privacy Team be notified in all instances there has been a data breach in order to conduct a risk assessment, even if the breach has been contained.

5.3 ***Stage 3: Containment and Mitigation***

The Industrial Registry will take immediate action locally to limit the breach e.g. securing information technology systems, recovering lost information, communication and instruction to staff to cease an activity, requesting an incorrect email recipient to delete all copies of the email (inbox and trash) and confirm they have done so.

The Privacy Team, in consultation with the Industrial Registrar/Deputy Industrial Registrar, will also take all reasonable steps to contain the breach and limit any further access or distribution of the affected personal information, including but not limited to:

- searching for and recovering data;
- confirming that no copies were made or confirming that the information was destroyed by the party receiving it;
- requesting ICTS to advise on and take action on any appropriate technological steps including:
  - remotely wiping a lost portable device;
  - shutting down impacted computer systems;
  - revoking access from relevant system users; and/or
  - changing passwords and system usernames.

If the breach involves a third-party (e.g. contractor or service provider), the Privacy Team will also consider involving them as soon as possible.

A preliminary fact-finding process will be conducted by the Privacy Team to initially determine the cause of the breach, the risk of spread, the nature of the personal information involved, options to mitigate, and the number and location of the affected individuals.

5.4 ***Stage 4: Assessment and documentation of the risks***

The Privacy Team are responsible for undertaking an assessment, building on the preliminary findings, to determine more detail around:

- What information was involved?
- Who was affected?
- How did the breach occur?
- Whether it is an eligible data breach under the IP Act.

This assessment will involve categorising the identified privacy breach as low, medium or high risk, according to the criteria below, and this decision is to be documented in the Register.

The relevant factors considered when assessing the severity of a breach resulting in serious harm to an individual, as outlined in the IP Act, include:

- the kind of personal information accessed, disclosed or lost;
- the sensitivity of the information;
- whether the personal information is protected by one or more security measures;
- if the personal information is protected by one or more security measures, the likelihood that any of those security measures could be overcome;

- the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information;
- the nature of the harm likely to result from the data breach; and
- any other relevant matter.

The assessment matrix, as outlined in the Procedure and replicated below, enables an assessment of the level of harm that may eventuate from the breach.

Event type	Low	Medium	High	Notifiable outside OIR/Industrial Registry
Loss or exposure of aggregated data only	X			Optional/voluntary to the affected individual and OIC/OAIC
Loss of individual level data where no real harm could occur e.g. paper files left behind after a meeting but quickly retrieved	X			Optional/voluntary to the affected individual and OIC/OAIC
Loss of a laptop or other device in a public place that is encrypted or password protected		X		Optional/voluntary to the affected individual and OIC/OAIC
Unintentional exposure of information to a third party where the third party has no malicious intent. i.e. an email to another member of the public service who has no interest in the data and has confirmed they have disposed of the email and attachments		X		Optional/voluntary but recommended to the affected individual
Loss or exposure of information is likely to result in serious harm e.g., physical, psychological, emotional, financial, or reputational harm including identity theft, assault, intimidation, financial loss, blackmail, extortion, threats to personal safety, inability to access funds, loss of employment opportunities etc.			X	Mandatory to the OIC/OAIC and the affected individual

For low and medium-risk breaches, the Privacy Team will work with the Industrial Registry and any required specialists (e.g. Risk Management and Cyber Security) to complete the steps in the Procedure.

For high-risk breaches, the Privacy Team will activate the Privacy Breach Response Team (Response Team) immediately and oversee the Procedure. The Response Team will consider the inclusion of various specialists (e.g. technology experts) to ensure the privacy breach is understood, properly assessed and handled.

For high-risk breaches, the Response Team will also, in consultation with the Industrial Registrar/Deputy Industrial Registrar, escalate the incident to the EDSCD, to allow for briefing of the Deputy Director-General, Director-General or the Minister. The Industrial Registrar/Deputy Industrial Registrar are to be included in any briefing communication. If the breach involves multiple agencies, the Response Team will liaise with those agencies

to determine those responsible for assessing the breach. For any type of criminal activity, such as theft, the Response Team will contact the Police.

Furthermore, if there is a risk that personal information could be used for identity theft or fraud, the Response Team may engage **IDCARE** - the National Identity and Cyber Support Service.

The Response team are to keep the Industrial Registrar/Deputy Industrial Registrar regularly informed of steps being taken and any responses or outcome of investigations.

5.5 ***Stage 5: Notification and communication***

In the case of an eligible data breach assessed as resulting in, or likely to result in, serious harm, the IP Act outlines that the OIC and the affected individual/s must be notified as soon as practicable and this will be the responsibility of the Privacy Team.

In the case of a breach involving a TFN, in accordance with the *Privacy Act 1988 (Cth)*, the OAIC and the affected individual/s are notified by the Privacy Team once the assessment has been completed.

Both of the above require mandatory notification via a statement produced and sent by the Privacy Team, in accordance with the templates outlined in the Procedure. In the case of multiple agencies being involved, or in the case of a breach by a contracted service provider, a joint notification statement will be made by those agencies involved.

In the case of low/medium risk breaches, depending on the circumstances, notification to OIC and affected individual/s is voluntary, however the Privacy Team have determined it would be best practice to do so.

The Privacy Team will determine the best course of action to notify affected individual/s, whether it be:

- directly to only those individuals at risk of serious harm;
- directly to all individuals whose personal information was lost or exposed; and/or
- by publishing a statement on the QIRC website for a period of at least 12 months.

5.6 ***Stage 6: Post-data-breach review and remediation – prevention of future breaches***

In the event of any data breach, the Industrial Registry will review and update its procedures and systems to mitigate the occurrence of similar recurrent breaches. For any high-risk breaches, any review will also take into consideration any recommendations given by the Privacy Team and any steps taken will be recorded by the Industrial Registrar/Deputy Industrial Registrar in an internal register for future reference. This may also involve increasing staff awareness and instigating further training where appropriate.

The Industrial Registry will work closely with the Privacy Team to ensure mitigation steps address the root cause of the breach, such as:

- a security audit and any modifications to physical controls such as locks, alarms;
- visitor access control;

- review of privacy policies and procedures;
- review of employee training and selection practices;
- a review of suppliers and third parties;
- updating passwords; and
- altered deployments of technology.

The Privacy Team will ensure all privacy breaches are recorded in the Register, and the Industrial Registry will maintain appropriate records, by way of an internal register, to provide evidence of how suspected privacy breaches are managed, including low, medium and high-risk privacy breaches. Tracking privacy breaches allows the Industrial Registry and the Privacy Team to monitor, analyse and review the type and severity of suspected and actual privacy breaches.

Further, the Industrial Registry and the Privacy Team will conduct an annual review of privacy breach response records and Register, to help identify and remedy:

- weaknesses in security or processes that are prone to error; and
- any deficiencies in the response procedure which impact on its effectiveness.

6. Register of Eligible Data Breaches and record keeping

All data breaches, whether considered an eligible data breach or not, must be documented and retained securely for audit and compliance purposes. The previously mentioned Register is a tool used to assist in the tracking and analysis of data breach risk as well as assessing the effectiveness of response methods.

The Privacy Team are the designated custodian of the Register and are responsible for its management and all reporting requirements associated with it.

Although not required by legislation, the Industrial Registry will maintain an internal register, in line with good record keeping practices, for internal tracking and analysis purposes.

7. Definitions, abbreviations, references and relating documents

7.1 For the purpose of this policy and response plan, the following definitions and abbreviations apply:

Term	Definition
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act.
Data breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
EDSCD	Executive Director Strategic Communication and Data

Term	Definition
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: • there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency, and • the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or • there has been loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and • the loss is likely to result in serious harm to any of the individuals to whom the information relates.
IDCARE	The national identity and cyber support service - www.idcare.org
ICTS	Information Communication Technology Services
Mandatory Data Breach Notification Scheme (MDBNS)	A framework that obliges Queensland public sector agencies to notify both affected individuals and the Office of the Information Commissioner (OIC) if they experience a data breach involving personal information that is likely to cause serious harm.
Mandatory notifiable data breach	A mandatory notifiable data breach occurs when an agency knows or reasonably suspects that unauthorised access/disclosure or loss of personal information has occurred and it is likely to cause serious harm to an individual. Once deemed eligible, the agency must notify both the Information Commissioner and the affected individuals under Chapter 3A of the *Information Privacy Act 2009.*
OAIC	Office of the Australian Information Commissioner
OIC	Office of the Information Commissioner
OIR	Office of Industrial Relations
Personal information	As defined in the *Information Privacy Act 2009*: *"...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."* Examples of personal information include: • name and contact details; • date of birth; • signature; • financial/bank details; • unique identifying numbers (i.e. TFN, driver licence number) • medical information; • occupation/employment history; • CCTV footage.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: • serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or • serious harm to the individual's reputation because of the access or disclosure
Staff member	A "staff member" includes an Industrial Registry Officer, a Member of the Court or Commission, or an Associate.

7.2 References and related legislation, policies, procedures and guidelines

Legislation

- *Information Privacy Act 2009*
- *Right to Information Act 2009*
- *Public Records Act 2023*
- *Human Rights Act 2019*
- *Privacy Act 1988 (Cth)*

Related Policy Framework

- *Industrial Registry Privacy Policy*
- *Office of Industrial Relations Privacy Policy*
- *Office of Industrial Relations Privacy Breach Response Procedure*
- *Office of Industrial Relations Cyber and Information Security Policy [internal]*
- *Code of Conduct for the Queensland Public Service*
- Queensland Government Information Security Classification Framework (v6.0.0) (effective November 2024)
- Queensland Government Information and Cyber Security Policy (IS18) (v9.0.0) (effective February 2025)
- Australian Government Protective Security Policy Framework (24 July 2025)

8. Contact

For further information, please contact the Industrial Registry:

By phone: 1300 592 987

By email: qirc.registry@qirc.qld.gov.au

By post: Industrial Registrar, Queensland Industrial Registry
GPO Box 373, Brisbane QLD 4001

In person: Level 21, Central Plaza 2
66 Eagle Street (Cnr Elizabeth and Creek Streets), Brisbane QLD 4000

Internet: www.qirc.qld.gov.au

9. Version Control

Version	Amendments	Approved	Date
1.1		M. Shelley, Industrial Registrar.	19 November 2025 (next review date: 19 November 2027)