Privacy breach response procedure

Version 1.1 | **Version effective:** 23/05/2025

Introduction

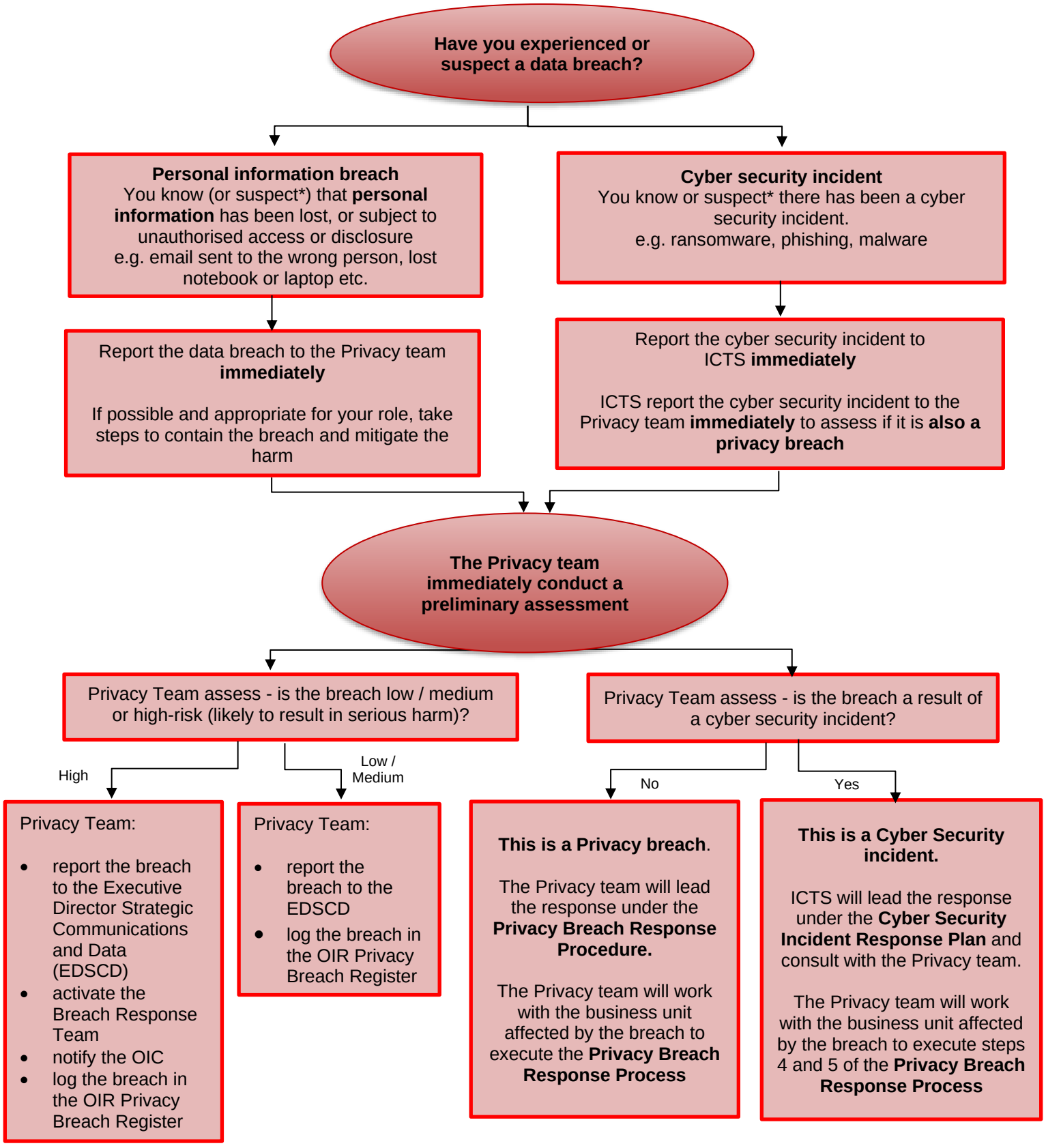
This Procedure outlines the Office of Industrial Relations' (OIR) planned response to privacy breaches, and suspected privacy breaches as required under section 73 of the *Information Privacy Act 2009 (Qld)*, (IP Act). It includes key actions and responsibilities to be followed in the event of a privacy breach.

Data can be at risk from cyber-attacks, ransomware, phishing, malware, system and process failure, human error, deliberate misconduct, lost or stolen devices and other risks. Not every cyber security incident will result in a privacy breach, and not every privacy breach will be as a result of a cyber security incident; for example, an email containing personal information erroneously sent to the incorrect email address will be a privacy breach but not be a cyber security incident, whereas an attack on the OIR's network that restricts the use of its system but doesn't involve any personal information will be a cyber security incident but not a privacy breach. Whenever an incident involves the potential exposure of 'personal information', it must be assessed as a privacy incident and it is also possibly a notifiable 'data breach'.

OIR follows a risk management approach to dealing with security and privacy threats. The Privacy team will evaluate all data breaches on a case-by-case basis to determine if personal information is involved and therefore a privacy breach has occurred. Actions will then be taken according to an assessment of risks and responsibilities in the particular circumstances.

Overview: procedure for all staff

This procedure sets out the steps to be followed where OIR experiences a data breach or suspects a data breach.



Reporting a breach

It is the responsibility of all staff at OIR to be aware of this Procedure and to report suspected privacy breaches as soon as possible. All privacy breaches reported to the Privacy team will be recorded in the OIR Privacy Breach Register.

Depending on the nature of the privacy breach, the law might consider it a 'notifiable data breach', meaning that the Office of the Information Commissioner (OIC) and the affected individuals (with very few exceptions) must be notified.

The Officer of the Australian Information Commissioner (OAIC) must be notified where Tax File Numbers are included in the privacy breach. The Privacy team will make an assessment about this, in accordance with the Privacy Breach Response Process outlined below.

Even if staff have contained the privacy breach (for example, retrieved a stolen laptop or lost hard-copy files), they must still tell the Privacy team. The Privacy team will assess any residual risk, and they can also consider whether further action is needed to avoid a similar occurrence.

Assessing the breach

The Privacy team will make a preliminary assessment of the risk posed to the individual/s affected by the privacy breach. This will involve assessing the privacy breach as low, medium or high-risk, according to the criteria below. The Privacy team will document this decision.

Event type	Low	Medium	High	Notifiable outside OIR
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

Event type	Low	Medium	High	Notifiable outside OIR
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 impacted business area and any required specialists (for example Risk Management and Cyber Security) to complete the steps in the Privacy Breach Response Process.

- For high-risk breaches, the Privacy team will activate the Privacy Breach Response Team immediately and oversee the Privacy Breach Response Process. The Breach Response Team will include various specialists from OIR to ensure the privacy breach is understood, properly assessed and handled.

- For high-risk breaches, the Privacy team will also escalate the incident to the Executive Director Strategic Communications and Data (EDSCD), to allow for briefing of the Deputy Director-General, Director-General or the Minister.

Overview: privacy breach response process

This process sets out the steps followed by the Privacy team/ Breach Response Team and the impacted business unit once a privacy breach has been reported to the Privacy team/Cyber Security.

1. Immediately take all reasonable steps to contain the breach

Containment may include:

- recalling the email if sent within the OIR
- contacting an external recipient to ask them to not deal with the email, delete it from their inbox and trash and confirm they have done this.

2. Assess and document the risks

Risk factors may include:

- the type of personal information involved, high risk information may include
  - health information
  - contact details
  - tax file numbers (TFNs)
- who is affected by the breach
- the cause of the breach
- how effective containment steps have been
- the likely harm to the affected individuals.

3. Review containment steps and remediate further if required

4. Notify and Communicate

Notification is made to affected individuals as appropriate and to the OIC / AOIC (if TFNs are involved) by the Privacy Team.

Communicate with staff and stakeholders about the breach, steps taken to date and status as required.

5. Prevent future breaches

Review for system improvements. Identify measures that can be taken to prevent similar breaches in the future. This may include targeted training and awareness, reviewing policy and procedure, technical security controls etc.

The privacy breach response process

This process sets out the steps to follow once a privacy data breach has been reported to the Privacy team or Cyber Security.

For low and medium-risk breaches, the Privacy team will assist the impacted business unit and oversee these steps. For high-risk breaches, the Privacy team will assist the impacted business unit, and the Breach Response team will oversee these steps. The Breach Response Team members are responsible for keeping their managers and Executive Directors informed about issues and escalate them as required throughout the execution of the Privacy breach response process.

Other OIR staff may be required to assist with the response process, by providing information, evidence, or changing technology settings. Any such action requested by the Privacy team or the Breach Response Team should be carried out without delay. Enquiries received about any data breach should be directed to the Privacy team in the first instance.

Step 1: Contain the privacy breach

- OIR will immediately take all reasonable steps to contain the privacy breach and limit any further access or distribution 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
  - requesting Information Communication Technology Services (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
    - changing passwords and system usernames.

  Understanding how the privacy breach occurred will help in identifying the appropriate steps to contain it.

- OIR will conduct preliminary fact-finding about the privacy breach.

  This will involve finding out the cause, risk of spread, and nature of the personal information involved in the privacy breach, options to mitigate, number and the location of the individuals affected.

  If the privacy breach involves a third-party vendor/supplier, OIR will consider involving them as soon as possible.

Step 2: Assess and document the risks to the individual/s affected

- For monitoring purposes, the Privacy team will notify the EDSCD of the breach.

- OIR will consider whether the privacy breach is likely to result in harm to any of the affected individuals. As soon as practicable, OIR will take remedial action to prevent or lessen the likelihood that the privacy breach will result in harm to any individual.

  This step may take place at the same time as the privacy breach is being contained and assessed. Remedial action will depend on the nature of the privacy breach but may involve recovering lost information before it is accessed or changing access controls on customer accounts before access to, or unauthorised transactions can occur.

- OIR will complete an assessment of the harm that may eventuate from the privacy breach.

  The assessment must determine whether there are reasonable grounds to believe that the privacy 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 assessment must be completed **as soon as practicable**, and at the very latest within 30 calendar days. **Ideally, the assessment should be done within 2-3 days**. The assessment must be documented.

  Note it may be necessary to commence Step 4 (Notify and communicate) before the assessment has been completed or the privacy breach is fully contained.

  - For high-risk privacy breaches, the Privacy Breach Response Team will consider whether to involve any other internal or external parties at this stage, for example:
    - If the privacy breach involves multiple agencies, OIR will liaise with the other agency / agencies to determine who will be responsible for assessing the privacy breach within the required period, and whether a joint response team should be formed.[1]
    - For other types of criminal activity (e.g. theft), OIR will contact the local police.

Step 3: 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 remediation steps possible will be taken on this basis.
- For high-risk breaches, if there is a risk that the personal information could be used for identity theft or other types of fraud, OIR may engage with IDCARE, the National Identity and Cyber Support Service, on 1800 595 170, or via www.idcare.org. IDCARE can offer OIR advice and can also assist affected individuals.

[1] See s.48(5) of the IP Act.

Step 4: Notify and communicate

Notification required by law

- Notification of privacy breaches to the OIC is **required under the IP Act** where there are reasonable grounds to believe it 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 the AOIC is **required under the federal *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 privacy 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 (i.e. low-risk and other medium-risk breaches). If we choose to voluntarily notify affected individuals, we do not need to notify the OIC, though it is best practice to do so.

Notification to affected individuals at risk of serious harm

There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable':

1. Directly notify only those individuals at risk of serious harm, or
2. Directly notify all individuals whose personal information was lost or exposed in the privacy breach
3. Publish the statement on an accessible agency website for at least 12 months.

Where it is possible to identify and contact only those individuals at risk of serious harm, the OIR must directly notify those individuals unless an exception 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
- if notification would compromise or worsen the agency's cyber security, or lead to further privacy breaches.[2]

The OIR might also publish the notification on our website.

Where it is not possible to identify which individuals might be at risk of serious harm, but it is possible for us to directly contact all individuals whose personal information was lost or exposed in the privacy breach, then the OIR will directly notify all individuals affected by the privacy breach. Publishing the notification more broadly, including on the OIR website, will be considered.

[2] See ss. 55, 58, 59, and 60 of the IP Act.

Where it is not reasonably practicable to identify which individuals might be at risk of serious harm, and it is not practicable to directly contact all individuals affected by the privacy breach (for example, if up-to-date contact details for old customers are not available), then a notification should be published on the OIR website for at least 12 months.[3] The OIR 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 will be used to provide information about the investigation, any updates and what further action individuals may take and what steps the OIR is taking to prevent any future privacy breaches. A media response should also be considered.

Notification to Information Commissioner/s by the Privacy team

Mandatory notification requires the Privacy team to prepare a statement in relation to a privacy breach involving personal information. This statement **will be sent to the Queensland Information Commissioner** (part of the OIC) **as soon as practicable by the Privacy team.**

In relation to a privacy breach involving TFNs, the statement **will be sent to the Australian Privacy Commissioner** (part of the OAIC) **as soon as practicable**.

If the privacy breach involves other agencies, and another agency was responsible for the assessment of the privacy breach, a **joint notification** should be made on behalf of all agencies, by the agency which conducted the assessment of the privacy breach,[4] and **will also be provided directly to affected individuals as soon as practicable**.

If the privacy breach involves a contracted service provider, a **joint notification** should be made on behalf of all organisations, by the organisation with the closest relationship to the affected individuals.[5]

Communication to staff and stakeholders

Steps for high-risk breaches

- Depending on the number of individuals affected, a dedicated webpage, and/or telephone line may be set up.
- Consideration will be given to whether third parties such as insurance companies, professional or other regulatory bodies, credit card companies, financial institutions or credit reporting agencies, other internal or external parties, such contractors, or outsourcing agencies should be informed. Consideration will also be given to groups

[3] See section 53 of the IP Act.
[4] See s. 56 of the IP Act.
[5] The notifiable data breach scheme applies if the data involved in the privacy breach was held directly by our agency, or if it was held on our behalf by a contracted service provider such that our agency was still in 'control' of the data; see s.13 of the IP Act.

which represent the affected individuals, such as the relevant union, if personal information about staff was compromised.

Step 5: 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.
- High-risk privacy breaches will be added to the OIR's internal register of eligible (i.e. notifiable / high-risk) privacy breaches.[6]
- Mitigation steps will address the identified root cause of the privacy 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
    - altered deployments of technology.
- For high-risk privacy breaches, a review of the process used with details of any recommendations, will be conducted after the process concludes, and saved for future reference.
- The Privacy team will ensure all privacy breaches are recorded in an OIR register, and instruct business units to maintain appropriate records, to provide evidence of how suspected privacy breaches are managed, including low, medium and high-risk privacy breaches. Tracking privacy breaches allows the OIR to monitor, analyse and review the type and severity of suspected and actual privacy breaches.
- The Privacy team will conduct an annual review of our privacy breach response records, to help identify and remedy:
    (i) weaknesses in security or processes that are prone to error
    (ii) any deficiencies in our response procedure which impact on its effectiveness.

Definitions

privacy breach means:

> *an incident in which there has been* **unauthorised access to, unauthorised disclosure of, or loss of, personal information** *held by (or on behalf of) the OIR*

[6] Section 72 of the IP Act.

Privacy breaches can or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harm to individuals and agencies. Although there is
overlap between cyber security incidents and privacy breaches, they are not exactly the same. Some cyber security incidents will not impact anyone's personal information. Some privacy breaches will involve only hard copy information such as paper files.

Examples of privacy breaches include:

- where a device containing personal information is lost or stolen
- where the OIR is subject to a malicious cyber-attack
- where personal information is mistakenly sent or provided to the wrong person.

personal information means:

information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion

This will include information about:

- our staff
- clients and employees of businesses
- employees, including prospective employees and contractors
- representatives and employees of businesses and organisations
- representatives of organisations, local governments and members of ministerial advisory committees (that may be constituted from time to time)
- vendors and service providers.

This information may include:

- name and contact details
- date of birth
- signature
- photographs
- financial/bank details including Centrelink and Veteran Affairs information
- unique identifying numbers (e.g. tax file number, driver licence number)
- cultural background
- medical/health/diagnostic information
- occupation and employment history
- details about persons making complaints, subjects of complaints and witnesses
- recruitment information, such as applications, curriculum vitae, referee reports, interview notes and selection panel assessments
- information about staff relevant to human resource management functions (e.g. leave entitlements, bank account details, superannuation information, pay scale)
- footage captured by camera surveillance systems or electronic monitoring devices in OIR premises, such as at regional offices

- information collected during the investigations, prosecutorial, review and appeals processes.

Individuals may still be identifiable even if steps have been taken to de-identify information (for example, removing direct identifiers or aggregating data). As such, it is prudent to treat de-identified information as personal information in the event of a data breach.

sensitive information means:

a specific category of personal information defined in schedule 5 of the IP Act. Sensitive information is information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation or practices
- criminal record
- health information
- genetic information that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification
- biometric templates.

notifiable data breach means:

a privacy breach which meets certain criteria, such as to trigger a legal requirement to notify the affected individuals, and/or appropriate regulator.

low-risk privacy breach means:

a loss or exposure of aggregated data only, or of individual level data in circumstances where it is reasonably believed that no real harm could occur (e.g. paper files are left behind in a meeting but quickly retrieved).

medium-risk privacy breach means:

a loss or exposure of personal information where it is reasonably believed that the third-party recipient does not have malicious intent, and that the data is somewhat protected (e.g. a laptop with encrypted data is left on a bus).

high-risk privacy breach means:

it is reasonably believed that the privacy breach is ***likely to result in serious harm*** to one or more of the individuals to whom the information relates (e.g. external hackers breach our firewall and copy valuable customer data). What we call a 'high-risk' privacy breach will be a 'notifiable' data breach, unless it falls under one of the exceptions to the notification rules.

serious harm means:

'serious harm' includes such things as serious physical, psychological, emotional, financial, or reputational harm. Examples of harms could include:

- identity theft
- assault
- intimidation
- financial loss
- inability to access funds or information
- blackmail
- extortion
- threats to personal safety
- loss of business or employment opportunities
- humiliation
- stigma
- embarrassment
- anxiety
- depression
- damage to reputation or relationships
- discrimination
- bullying
- marginalization
- other forms of disadvantage or exclusion.

likely to result in serious harm means:

the risk of serious harm to an individual is more probable than not. To help assess the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure.

Content owner, endorsement and review date

Document owner	Right to Information and Privacy
Policy approved by	OIR Executive Leadership Committee
Date policy approved	30 April 2025
Review date	29 April 2027

Metadata

Description (paragraph on subject matter and intention)	The Office of Industrial Relations (OIR), collects and manages the personal information of clients, customers, licensees, business partners, contractors, their representatives, and staff, to carry out its functions. The purpose of this policy is to help OIR users understand what personal information is and how the OIR will handle it.
Division/Directorate	Strategic Communications and Data
Content owner (role)	Manager, Right to Information and Privacy
Business Unit responsible	Right to Information and Privacy
Key words (as many as possible)	Privacy, personal, information, sensitive, compliance, Information Privacy Act, IPOLA Act, IP Act Data, Breach, response, plan, mandatory, notification, eligible, lost data, unauthorised access, identity, TFN, tax, file, number, Office of the Information Commissioner, Australian Information Commissioner.
Next review date	29 April 2027