Policy

DATA BREACH POLICY

Policy statement

The Department of Women, Aboriginal and Torres Strait Islander Partnerships and Multiculturalism (DWATSIPM) (the department) is committed to ensuring that data breaches are handled in accordance with the *Information Privacy Act 2009* (Qld) (IP Act), and the Mandatory Notification of Data Breach[1] (MNDB) scheme requirements.

The MNDB scheme requires agencies to respond promptly to suspected eligible data breaches by taking reasonable steps to contain the breach and mitigate harms, and to conduct timely assessments. The scheme also requires agencies to:

- publish a Data Breach Policy (section 73 of the IP Act) outlining how the department will respond to a data breach, including a suspected 'eligible data breach'
- establish and maintain an internal Register of Eligible Data Breaches
- notify the Information Commissioner, and particular individuals, of eligible data breaches.

Definitions of information privacy terms, including those related to data breaches, have been provided at Appendix A.

This Data Breach Policy will be reviewed every two years, or following times of significant organisational change, to ensure its continued relevance and appropriateness.

Objective

This policy aims to establish the department's approach to managing data breaches and complying with the Mandatory Notification of Data Breach[1] (MNDB) scheme requirements.

Scope

This policy applies to all DWATSIPM employees, and employees engaged on a temporary, part-time or casual basis, or on secondment from another department, as defined by the *Public Sector Act 2022 (Qld),* who handle personal information.

The 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, the department will carefully examine whether the information is considered to be 'held' by the department, by considering all relevant circumstances, such as the department's relationship with the information and relevant legislation and guidelines.

[1] *Information Privacy Act 2009, Chapter 3A*

Queensland Government

Stages for managing data breaches

The six key stages for managing and responding to data breaches are:

1. Preparation
2. Identification
3. Containment and mitigation
4. Assessment
5. Notification
6. Post-data breach (PDB) incident review and remediation.

A diagrammatic representation of these stages is provided in Figure 1:

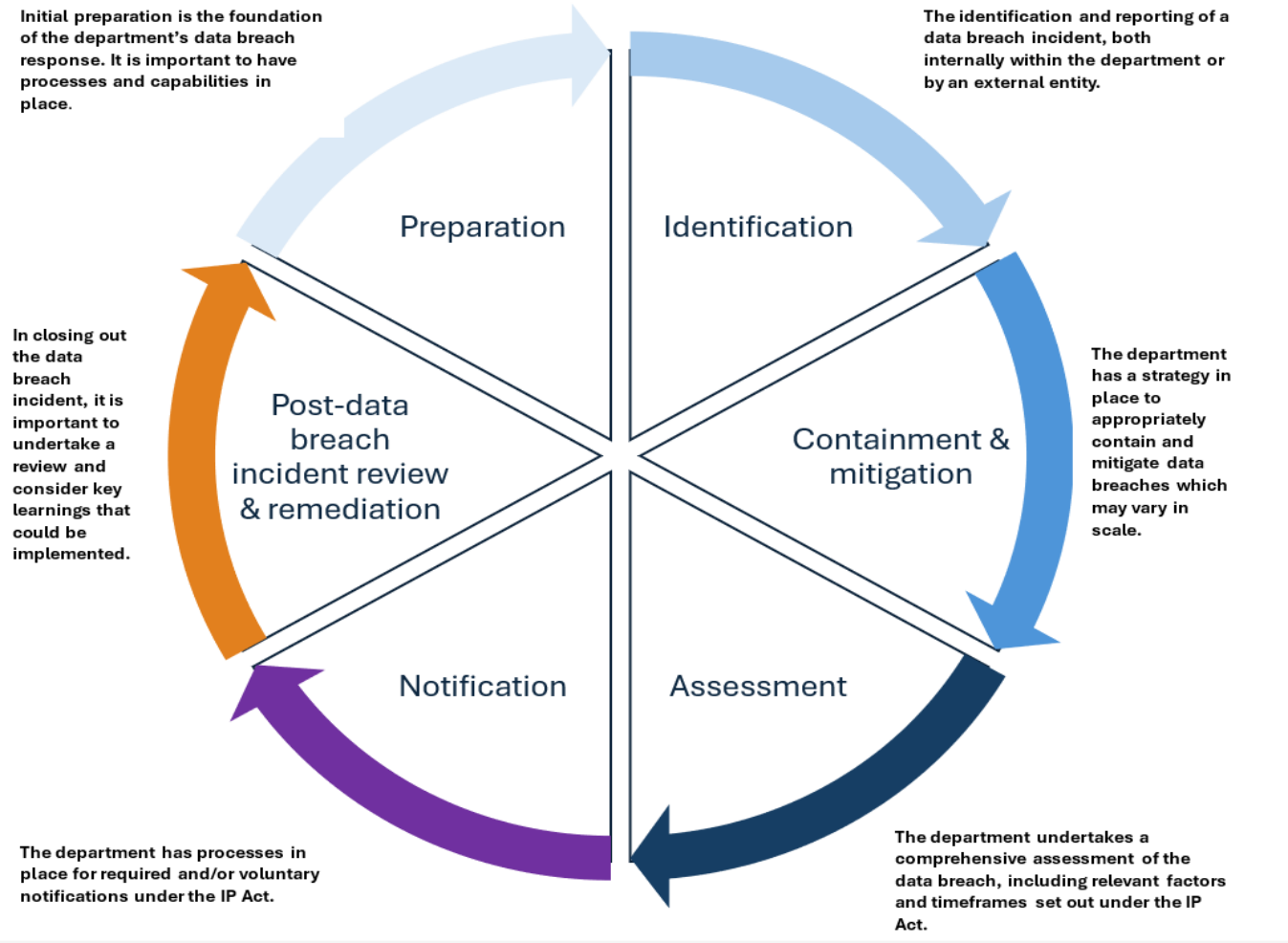
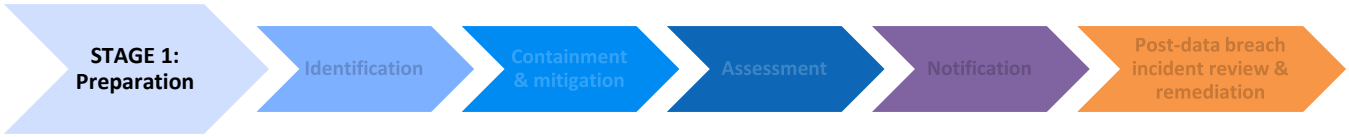


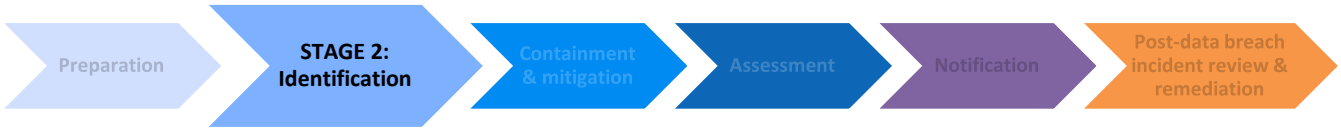
Figure 1: Key stages for managing and responding to data breaches



1. Preparation

The department proactively plans for responding to data breaches by:

- ensuring that the Data Breach Policy, which includes the process for responding to data breaches, is reviewed and updated regularly
- identifying and assessing privacy risks
- ensuring strong security measures are in place such as encryption, multi-factor authentication, and regular software updates
- promoting staff awareness and providing staff training on information security, including cybersecurity, and privacy.



2. Identification

Data breaches can be caused or exacerbated by a number of factors, and as a result, there is no single way that the department will respond to a data breach if one occurs. Each breach will be dealt with by the department on a case-by-case basis, with the department undertaking an assessment of the risks involved, and using that risk assessment (Appendix C) as the basis for deciding what actions to take in the circumstances.

What is a data breach?

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.

Personal information is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.

A data breach can happen in various ways. This includes malicious actions of third parties, internally due to human error, or a failure in information handling or security systems. However, not all data breaches will be an Eligible Data Breach and engage the MNDB.

What is an eligible data breach?

An **Eligible Data Breach** under the IP Act **always involves personal information** and may occur internally within an agency or involve the unauthorised access and/or disclosure of personal information by or to external parties, including threat actors or contractors.

Where a data breach involves personal information and any impacted individuals **may be seriously harmed**, then the data breach may be an **Eligible Data Breach**.

For a data breach to be an 'eligible data breach', which triggers notification and other obligations under the MNDB scheme, both of the following must apply:

- there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and

- the unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual') [2].

Serious harm

The harm which can potentially arise from a data breach will vary based on the nature of the personal information involved and the context of the breach.

Serious harm is defined in schedule 5 of the IP Act as including:

- 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.

Internal escalation and reporting of actual or suspected data breaches

The process for reporting and escalating data breaches, including eligible or suspected eligible data breaches, is as follows:

- the senior management responsible for the area in which the breach occurred, and the Manager, GPR, via the privacy@dsdsatsip.qld.gov.au mailbox, should be informed immediately about the breach
- other senior personnel responsible for information security, communications, legal services, human resources, and employee misconduct (e.g. Manager, Ethical Standards), should also be notified, as appropriate.

3. Containment and mitigation

Where the department knows about, or reasonably suspects a data breach, it immediately takes, and continues to take, all reasonable steps to contain the data breach and minimise the harm caused by the data breach.

These steps include:

- making efforts to recover the personal information
- securing and restricting access to breached systems, or shutting them down
- suspending the activity that led to the data breach, or revoking or changing access codes or passwords
- identifying specific roles and responsibilities of key officers in containing and mitigating the specific risk
- considering other stakeholders, as referenced in the department's information privacy and information security policies and procedures (Appendix B – Key Contacts and Stakeholders), that may be impacted by a data breach to ensure that all necessary areas of the department are involved and aware of the potential impacts of a data breach.

If a third party is in possession of the personal information and declines to return it, it may be necessary to seek legal advice on what action can be taken to recover the information. When recovering information, the department takes steps to ascertain whether the information has been shared or disseminated, and ensures copies have not been made or that all copies are recovered.

The department ensures that while containing an eligible, or suspected eligible, data breach, that information that may be required as part of an internal or external investigation into the breach, is not destroyed.

[2] *IP Act 2009 s47*

Initial evaluation

An initial evaluation of the actual or suspected data breach will be undertaken by a person of sufficient authority where the suspected data breach had occurred, in order to inform containment and mitigation strategies. This includes a risk assessment process (Appendix C), covering low, medium, high and extreme risk data breach scenarios.

Regardless of whether the breach is a low risk (small scale/minor) or a medium to higher risk (more significant/Suspected Eligible Data Breach), each risk level will require a different approach, especially in the context of containment and mitigation and notification obligations.

The department's risk assessment (Appendix C) will be informed by the following key elements:

- nature and sensitivity of information
- amount of information and number of affected individuals
- ease of identifying the individuals
- seriousness of the harm
- existing mitigating measures.

4. Assessment

If the department does not know, but reasonably suspects that a data breach is an eligible data breach, it will assess whether there are reasonable grounds to believe it is an eligible data breach. This assessment is to be **completed within 30 calendar days**, **unless the assessment time is extended under section 49 of the IP Act.**

The department's assessment and reasons for its decision as to whether a data breach is an eligible data breach are recorded in writing, and include the material facts of the specific breach. The assessment addresses the section 47(2) matters detailed under the 'Serious harm' section of this policy, and any other relevant factors.

Extension of time to assess a breach

If the department is satisfied that it will not be able to complete the assessment in 30 calendar days, it can extend that time under section 49.

Data breaches affecting another agency

If the department becomes aware that an eligible, or suspected eligible, data breach may affect another agency, it will give the other agency a written notice of the data breach that includes a description of the:

- data breach, and
- kind of personal information involved in the data breach, without including any personal information in the description.

5. Notification

If the department reasonably believes that there has been an eligible data breach involving personal information held by the department, it will:

- prepare a statement which includes the information stated in section 51(2)
- give the statement to the Information Commissioner,
- notify any individuals affected by the breach, including the information stated in section 53(2)
- notify other entities as appropriate, or where required.

Notifying the Information Commissioner

Unless an exemption applies, the department will notify the Information Commissioner as soon as practicable, in writing, after forming the belief that a data breach is an eligible data breach.

Notifying particular individuals

There is no requirement to notify individuals whose personal information is not involved in a data breach. However, if the department identifies an individual who is likely to suffer harm for reasons other than their personal information being involved, the department will notify these individuals if it is possible to do so without the risk of further breaches, as this may assist in mitigating any risk of harm.

Unless an exemption applies, as soon as practicable after forming a reasonable belief that a data breach is an eligible data breach, the department will take the steps set out in section 53 to notify particular individuals and provide them with the information required in section 53(2).

Section 53 provides three options for notifying individuals, depending on what is reasonably practicable in the circumstances. Whether an option is reasonably practicable will depend on a consideration of factors, including the:

- time, cost and the effort required to notify affected individuals
- currency and accuracy of their contact details, which will affect the ability of the agency to notify the affected individuals (noting, however, the mechanism for confirming the contact details and other information of affected individuals prescribed in section 54).

Option 1: Notify each individual

If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, the department will take reasonable steps to notify each individual of the required information.

Option 2: Notify each affected individual

If Option 1 does not apply, the department will take reasonable steps to notify each affected individual of the required information for the data breach, if doing so is reasonably practicable.

Under section 47(1)(a)(ii) and (b)(ii), an ‘affected individual’ is someone:

- to whom the personal information relates, and
- who is likely to suffer serious harm as a result of the data breach.

An individual will be an affected individual if the information involved in an eligible data breach is about them, regardless of whether it was originally collected from the individual or a third party.

It is possible that a privacy complaint may arise as a result of the notification to affected individuals, and in these circumstances the department will respond to the complaints in line with the customer complaint management policy.

Note: Notifying children
Where a data breach involves the personal information of a child, notification will generally be made to the child's parent or legal guardian.

For minors aged 16 years or older, it may be appropriate to make the notification directly to the child.

Option 3: Publish information

If options 1 and 2 do not apply, the department will publish the required information on an accessible departmental website for a period of at least 12 months. The department is not required to include information in its notice if it would prejudice its functions.

For public notification via the department's website, the notification will include a description of the kind of personal information involved in the data breach, **without** including any personal information in the description.

Notifying other entities

In some circumstances it may be appropriate, or it may be required, to notify other entities of a data breach. This includes the following:

- If the breach involves 'corrupt conduct' within the meaning of the *Crime and Corruption Act 2001* (Qld), the Crime and Corruption Commission Queensland must be notified.
- Requirements to report cyber and information security incidents to Queensland Government Information Security Virtual Response Team, according to the Business Impact Level.
- If the breach involves a cyber security incident that results in a loss and the entity is an agency covered by the Queensland Government Insurance Fund (QGIF), QGIF should be notified.
- If the breach appears to involve theft or other criminal activity, the Queensland Police Service (QPS) should be notified as a matter of course. The QPS website has links and assistance to report cybercrime and other offences.
- If the breach involves the loss or unauthorised destruction of a public record, an entity subject to the *Public Records Act 2023* (Qld) must notify the State Archivist.
- Entities with obligations under the *Privacy Act 1988* (Cth) National Data Breach (NDB) scheme (e.g. Tax File Number recipients) may be obliged under the NDB scheme to report the breach to the Office of the Australian Information Commissioner.

Depending on the circumstances of the data breach and the information involved, other notifications may be appropriate. For example, the portfolio's Minister, financial institutions, or credit card companies, or professional or other regulatory bodies.

Exemptions from notification obligations

In accordance with Chapter 3A, part 3, division 3 of the IP Act, the circumstances in which the department is not required to comply with the notification obligations, include those where:

- complying with the obligation would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal
- the eligible data breach involves more than one agency, and another agency is undertaking the notification obligations
- the department has taken specified remedial action under section 57
- compliance would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information
- compliance would create a serious risk of harm to an individual's health or safety, and

- compliance is likely to compromise or worsen the department's cybersecurity or lead to further data breaches of the department.

A number of these exemptions have limitations or impose additional obligations. Refer to the ***MNDB Exemptions*** *guideline* for more information.

The notification obligations and considerations may apply to *any* breach or compromise of *any* type of information, and not only to those assessed as eligible data breaches under the MNDB scheme.

Record-keeping requirements

- The department maintains an internal register of eligible data breaches in line with the Data Breach Policy and the MNDB scheme.

6. Post-data breach incident review and remediation

To prevent future data breaches, the department undertakes a PDB incident review of the process that was used for the data breach, after it has been handled. The report includes a high-level overview of the process adopted to conduct the PDB incident review and remediation, analysing all aspects of the data breach to identify key learnings. This analysis includes details of remediation activities, the process for conducting the PDB incident response assessment, and the effectiveness of the Data Breach Policy.

Roles and responsibilities

Roles	Responsibilities
Director-General	• The Director-General is ultimately accountable for the department's compliance with privacy legislation and for managing data breaches.
Executive Leadership Team	• Review and monitor reports on information privacy risks and data breaches.
Deputy Director-General, Corporate Services	• The Deputy Director-General, Corporate Services, who is the department's Privacy Champion, is responsible for: – promoting a culture of privacy within the department that values and protects personal information, including the understanding of the importance of managing and reporting data breaches in line with the MNDB Scheme.
Managers, Directors, Executive Directors, and Deputy Directors-General within Divisions and Branches	• Managers, Directors, Executive Directors and Deputy Director-Generals within Divisions and Branches are responsible for responding to data breaches within their relevant business areas. This includes: – assessment of suspected data breaches – notifying affected individuals in line with the Data Breach Policy – maintaining Divisional Breach Registers – evaluating the effectiveness of the breach response.

Roles	Responsibilities
Governance, Planning and Reporting Team (GPR)	• The GPR team is responsible for co-ordinating the development, and overseeing the department-wide implementation, of the Data Breach Policy. This includes: – developing, maintaining, testing and updating the Data Breach Policy – maintaining an Eligible Data Breach Register – providing advice and support to business areas in implementing the Data Breach Policy.
Incident Response Team (IRT)	• The Incident Response Team (IRT) is a temporary team consisting of senior DWATSIPM officers responsible for co-ordinating and managing the department's response to a data breach, including assessing and responding to the data breach, providing executive updates, conducting reviews, and ensuring compliance with organisational frameworks and legislative requirements. • Depending on the nature of the breach, the IRT (in instances where it is necessary to convene the response team), may need to include additional staff as external experts, e.g. an IT specialist, data forensics expert or a human resources advisor.
Information Services, DFSDSCS	• Manage technical containment and investigations of ICT-related breaches in accordance with the MoU between DWATSIPM and DFSDSCS for the delivery of Corporate Services
Human Resources and Ethical Standards	• Reviewing and updating the information privacy and information security online training courses
All staff	• All staff are responsible for: – complying with the IP Act, including protecting personal information held by the department from unauthorised access, disclosure or loss – promptly reporting any actual or suspected data breaches to their supervisor.

Human Rights

The policy has been reviewed for compatibility with human rights under the *Human Rights Act 2019* (the Act). The policy was not found to engage any human rights under that Act. As such, it is reasonable to conclude the policy is compatible with human rights.

Authority

Information Privacy Act 2009 (Qld)

Right to Information Act 2009 (Qld)

Information Privacy and Other Legislation Act 2024 (Qld)

Invasion of Privacy Act 1971 (Qld)

Crime and Corruption Act 2001 (Qld)

Police Powers and Responsibilities Act 2000 (Qld)

Police Service Administration Act 1990 (Qld)

Public Interest Disclosure Act 2010 (Qld)

Public Records Act 2023 (Qld)

Public Sector Ethics Act 1994 (Qld)

Public Sector Act 2022 (Qld)

Human Rights Act 2019 (Qld)

Victims' Commissioner and Sexual Violence Review Board Act 2024 (Qld)

Delegations

Not applicable

Records File No:

Date of approval: July 2025

Date of operation: July 2025

Date to be reviewed: July 2027

Office: Governance, Planning and Reporting

Help Contact: Manager, Governance, Planning and Reporting
privacy@dsdsatsip.qld.gov.au

Links:

Related Policies and Procedures

- Acceptable use of ICT services facilities and devices policy (internal)
- Acceptable use of ICT services facilities and devices procedure (internal)
- QGEA Information security incident reporting standard (internal)
- QPP Privacy Policy
- QPP Privacy Procedure
- Data Breach Response Plan Procedure (internal)
- Data Governance Policy and Procedure (internal)
- Information Security Management System (ISMS) Directive (internal)
- DTATSIPCA Information Security Policy (internal)
- Information Security: Incident Response Plan (internal)
- Generative AI Guidelines (internal)
- Enterprise Risk Management Framework (internal)
- Enterprise Risk Management Policy (internal)
- Enterprise Risk Management Procedure (internal)
- Queensland Government – Information Security Policy (IS18:2018) (internal)
- Records Governance Policy (internal)
- Records Governance Procedure (internal)

Related Standards

- Queensland Government Information Standard (IS44 Information Asset Custodianship)
- Queensland Government Information Standard (IS18 Information Security Management System)
- ISO/IEC 27001:2022 – Information security management systems
- AS ISO 31000:2018 Risk Management – Guidelines

Appendix A – Definitions

Term	Meaning
Agency Worker	A person who carries out work in any capacity for an agency as defined in section 7 of the *Work Health and Safety Act 2011* (Qld), including work as: (a) an employee (b) a contractor or subcontractor or an employee of a contractor or subcontractor (c) an apprentice or trainee (d) a student gaining work experience, or (e) a volunteer.
Affected individual	An 'affected individual' is someone: • to whom the personal information relates, and • who is likely to suffer serious harm as a result of the data breach.
Australian Information Commissioner	The Australian Information Commissioner.
Commonwealth Privacy Act	The *Privacy Act 1988* (Cth).
Contracted Service Provider	A Contracted Service Provider (CSP) is an external organisation or entity engaged by a government agency to perform certain functions or activities on its behalf. If these arrangements involve handling personal information, the agency must ensure the CSP complies with privacy principles under the *Information Privacy Act 2009 (Qld).* This means the agency is responsible for taking reasonable steps to ensure the CSP protects personal information in line with the legislative requirements.
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.
Data Breach Policy	The Data Breach Policy aims to establish the department's approach to managing data breaches and complying with the Mandatory Notification of Data Breach (MNDB) scheme requirements.
Data Breach Response Plan Procedure (internal)	The purpose of the Data Breach Response Plan Procedure is to outline the process to be followed by DWATSIPM staff in the event that the department experiences a data breach, or suspects that a data breach has occurred within the department. It is a more detailed, internal procedural document complementing the Data Breach Policy, which details the department's more specific processes in managing and responding to a data breach.

Term	Meaning
Disclose	Section 23 (1) of the IP Act, defines the disclosure of personal information as: (1) An entity (the ***first entity***) ***discloses*** personal information to another entity (the ***second entity***) if— (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: (a) 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** (b) 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.
Information Commissioner	The Queensland Information Commissioner.
Incident Response Team	A temporary team formed to assess and respond to data breaches, provide executive updates, conduct reviews, and ensure compliance with organisational frameworks and relevant legislative requirements
IP Act	The *Information Privacy Act 2009* (Qld)
***Held* or *hold* in relation to personal information**	Personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (a) whether the information or opinion is true or not, and (b) whether the information or opinion is recorded in a material form or not.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.

Term	Meaning
Use	Section 23 (2)(3)(4) of the IP Act, defines the **use of personal information** as: (2) An entity ***uses*** personal information if it— (a) manipulates, searches or otherwise deals with the information; or (b) takes the information into account in the making of a decision; or (c) transfers the information from a part of the entity having particular functions to a part of the entity having different functions. (3) Subsection (2) does not limit what actions may be ***use*** of the personal information. (4) However, ***use*** of the personal information does not include the action of disclosing the personal information to another entity.
TFN	A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.

Appendix B – Key Contacts and Stakeholders

Organisation/Position	When to contact and contact details
Crime and Corruption Commission	If the breach involves corrupt conduct within the meaning of the *Crime and Corruption Act 2001* Phone: 07 3360 6285 (Executive Direction, Integrity Services) https://www.ccc.qld.gov.au/public-sector/assessing-and-notifying
Office of the Australian Information Commissioner	If the breach involves Tax File Numbers (TFN) or if any obligations under the *Privacy Act 1988* (Cth) apply https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-adata-breach/
Queensland Government Information Security Virtual Response Team (QGISVRT)	Privacy breaches involving cyber security incidents, ICT systems or with broader implications for OIC Phone: 07 3215 3951 Email: qgisvrt@qld.gov.au
Queensland Government Insurance Fund (QGIF)	Privacy breaches involving a cyber incident that results in a loss and OIC is considering making a claim https://qgif.qld.gov.au/
Queensland Police	Privacy breaches that appear to involve theft or other criminal activity. QPS has links and assistance to report cybercrime.

Appendix C – Risk Assessment

The following tool may assist in assessing the impact of a privacy breach by 'risk scoring'. Risk scoring is achieved when you multiply the *probability* against the *impact.*

Impact Criteria

When assessing impact look at the actual impact and damage to the individual concerned

	Impact Criteria			
	Harm to Individual(s)	**Reputational harm to DWATSIPM**	**Cost**	**#**
Insignificant	No harm to individuals	Nil or minor impact on reputation. Unlikely to be reported in the media.	Trivial impact on budget <$1000	1
Minor	No or little harm to individuals, which could include minor inconvenience or disruption to their activities	Small impact on reputation, may be some local news reports for 1-2 days	Minor impact on budget <$10k	2
Moderate	Likely harm to individuals that would require them to take some action or ensure their welfare is not impacted	Moderate impact on reputation sustained regional and/or national negative perception	Moderate impact on budget <$100k	3
Major	Harm to individuals which has impacted on their safety and will need to action to protect their interests	Sustained regional and/or national negative perception	Significant cost impact on budget<$500k Remediation is likely to be time consuming and complex	4
Critical	Individuals suffer harm which requires them to take action to protect their safety or financial security	Sustained negative national perception	Large cost impact on budget >$500k Remediation is likely to be time consuming and complex	5

Likelihood Criteria

When assessing likelihood, assess what is the probability of the breach happening again.

Likelihood Criteria		
Rare	One off incident – will not be repeated	1
Unlikely	May happen again, but remedial actions make this unlikely	2
Possible	Could happen again but remedial action reduced this likelihood	3
Likely	Is likely to happen again with 1-7 days unless action is taken	4
Almost certain	Is likely to happen again almost immediately unless action is taken ASAP	5

The Matrix

	Consequence				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Critical**
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

Source: OIC privacy breach matrix