Effective Date: 26/09/2025 Version: 1.0

4.9 – Information Privacy Data Breach

Responsible Owner: Director, Legal Services Branch

Audience: ☒ SCSD ☒ State Ops ☒ QFR ☒ RFSQ

1. Purpose

Queensland Fire Department (QFD) is required to manage personal information in compliance with the *Information Privacy Act 2009* (Qld) (IP Act). The IP Act contains a Mandatory Notification Data Breach (MNDB) scheme which is applicable to all Queensland public sector agencies that are subject to the IP Act. This includes QFD.

Chapter 3A, section 73 of the IP Act requires QFD to prepare, and publish on its website, a data breach policy and notify the Office of the Information Commissioner (OIC), Queensland and affected individuals in the event of an eligible data breach.

This policy sets out the steps to be taken by QFD in the event of a data breach, specifically one that compromises the personal information of individuals. This policy focusses on the following six distinct stages:

- Stage 1: Preparation.
- Stage 2: Identification.
- Stage 3: Containment and mitigation.
- Stage 4: Assessment.
- Stage 5: Notification.
- Stage 6: Post-data breach review and remediation.

This policy supports QFD's compliance with the MNDB scheme and has been developed in line with the IP Act and guidance from the OIC.

2. Scope

This policy applies to all QFD permanent full time, part time, volunteer, trainee and temporary employees, contractors, consultants, third-party suppliers, vendors, and hosted manged service providers authorised to access, manage, process or store QFD information assets and systems.

Compliance with this policy is mandatory.

3. Definitions

Refer to Appendix A for all definitions relevant to this policy.

4. Roles and responsibilities

All QFD employees have a responsibility to ensure personal information they handle in the performance of their duties is managed in accordance with the IP Act.

Below is a list of the roles and responsibilities of QFD officers and internal business units involved in responding to data breaches.

Role	Responsibility
Commissioner	The Commissioner provides strategic leadership, oversight, and accountability for QFD's data breach policy, ensuring compliance, effective incident response, and continuous improvement.
Managers, Supervisors, and Senior Management (including the Executive Leadership Team)	All levels of management within QFD are responsible for taking immediate steps to: • identify and escalate concerns within area of responsibility which may enliven the requirements of this data breach policy. • report a data breach that is also a cyber security incident to the Executive Director, Information and Technology Directorate, if not already reported.

Role	Responsibility
Employees, volunteers, consultants, contractors, and managed service providers	All employees, volunteers, consultants, contractors and managed service providers are responsible for: • recognising a data breach and promptly reporting it • only collecting or using personal information in accordance with QFD's 'Queensland Privacy Principles – Privacy Policy' (QPP Policy) • restricting access to information only to those that require it for their role • only keeping information for the length of time necessary in accordance with the retention and disposal schedules • understanding their obligations under all relevant legislation, policies, procedures and guidelines, including the Code of Conduct for Queensland Public Service.
Information Asset Custodian	An Information Asset Custodian is the recognised officer responsible for implementing and maintaining information assets to the rules approved by the Information Asset Owner as per the QFD Information Asset Management Policy (P4.3) and the Information Asset Custodian Delegation of Responsibilities.
Right to Information (RTI) and Privacy Unit	The RTI and Privacy Unit is the central area to be contacted for all data breaches containing personal information and is responsible for: • QFD's Data Breach Response Plan, notification forms and templates, and central breach register (including the eligible data breach register) that will be used to manage and record details of the incident. • assessment of data breaches containing personal information • coordinating notification of eligible data breach to the OIC and affected individuals • educating employees about data breaches and recommending improvement to processes that will reduce the risk of future incidents • reviewing and updating QFD's QPP Policy and this Data Breach Policy.
Cyber Information Security	Cyber Information Security is a team within QFD's Information Technology Directorate which is responsible for managing and maintaining QFD's Information Security Management System in accordance with the Queensland Government Information Security Policy (IS18:2018). In addition to the above, the Cyber and Information Security team is responsible for: • notifying the RTI and Privacy Unit where an actual or suspected breach may involve personal information • assist with the appropriate and necessary containment measures, root cause eradication and post breach review. • providing guidance and training to employees on best practice for cyber security.
Conduct Investigations Unit	The Conduct Investigations Unit is responsible for investigating an incident to determine whether serious misconduct or corrupt conduct has occurred or whether the reporting of an incident may be a public interest disclosure under the *Public Interest Disclosure Act 2010*.

5. How QFD prepares for a data breach

The following established processes demonstrates how QFD is prepared to respond to a data breach:

- **Maintaining a record of personal information held within QFD**

QFD has a comprehensive information asset register that lists the kind of information captured and what systems and databases store this information.

- **Restricting access to personal information**

QFD restricts access to the systems and software platforms containing personal information on a needs-only basis. By limiting the access of personal information to those who need the information to be able to perform their role provides a crucial step in reducing the potential for unauthorised access or disclosure.

- **Robust security framework**

QFD is committed to embedding strategic, consistent and structured enterprise-wide Information Security Management System (ISMS) which aligns to the Queensland Government Information Security Policy (IS18:2018) which requires all government agencies to implement an ISMS based on ISO27001 and that agency executives confirm the appropriateness of agency information security.

- **Information governance structure**

QFD maintains a comprehensive Information Management Policy Framework which is required to provide governance for QFD staff and volunteers on how to meet the information management and security objectives of the department. Additionally, QFD has committed to meeting the requirements of the Queensland Government's Information Asset Custodianship Policy (IS44:2013) by implementing an information asset management policy and information asset register. QFD's information governance structure also ensures information is protected in accordance with IS18:2018 and that records are disposed of in accordance with the *Public Records Act 2023*.

- **Regularly reviewing and updating our privacy practices**

In response to continuing advancements in technology and new emerging privacy threats, QFD continues to integrate privacy considerations into the development of new systems and programs that involve personal information, embedding data protection from the beginning.

QFD continues to review its privacy practices, including privacy collection notices and training/awareness materials to ensure they are current and operate in line with best practice. These actions will assist QFD in fulfilling its legislative obligations in managing personal information and preventing data breaches.

- **Education on breach prevention and identification**

QFD staff play a critical role in data breach preparation measures. QFD have developed cyber security awareness training program designed to teach staff the fundamentals of cyber security. Additionally, privacy awareness information is available to QFD staff to provide guidance to staff on how to uphold QFD's privacy compliance obligations.

6. Responding to a data breach

6.1. Stage 1: Identification of a data breach

The definition of a data breach is provided in Appendix A – Definitions.

A data breach can happen in various ways. Examples can include:

Malicious or criminal attack

- cyber incidents such as ransomware, malware, hacking, phishing or access attempts resulting in access to, leakage or theft of personal information
- social engineering or impersonation leading into inappropriate disclosure of personal information
- insider threats from employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions
- theft of a physical asset such as a paper record, laptop, removable storage device or mobile phone containing personal information.

System fault

- where a software bug allows access to a system without authentication, or results in automatically generated notices including the wrong personal information or being sent to incorrect recipients.

Human error

- when a letter or email is sent to the wrong recipient
- when system access is incorrectly granted to someone without appropriate authorisation
- when employees fail to implement appropriate password security, for example not reviewing access permissions, securing passwords, or sharing passwords and log in information.

Under the IP Act, an eligible data breach occurs when there is a data breach involving personal information and the data breach is likely to result in serious harm to an individual to whom the personal information relates.

QFD is required to have processes in place for detecting and identifying data breaches, including internal communication processes for considering and escalating a data breach (where necessary).

When a data breach is identified, the QFD RTI and Privacy Unit will be notified, along with officers from other business units within QFD such as:

- Information Technology
- Human Resources
- Legal Services

- Media, Communications and Online
- Finance and Procurement
- Internal Audit

The relevant business area that identified the data breach or was made aware of the data breach (if the data breach occurred externally) will commence completing QFD's data breach notification form. The content of the data breach notification form will assist in informing QFD's assessment to determine whether the MNDB scheme is to be engaged.

6.2. Stage 2: Containment and mitigation

In consultation with the relevant Information Asset Custodian and other relevant subject matter experts, QFD will immediately take steps to initiate a process of containment. This could include:

- stopping the unauthorised process
- recovering any records or data
- shutting down the system that was breached (or where system shut down is not practical, account privileges are to be restricted).

In addition to the above measures, QFD will also consider whether any of the following containment measures are required:

- identification of what happened to cause the incident
- establish if interim controls be implemented
- determine how serious the incident is (i.e. what information and individuals are impacted)
- does QFD need to work with any third parties to investigate and resolve the incident
- is internal assistance from other business areas required (i.e. information technology)
- whether the personal information can be recovered
- whether the person who has received information incorrectly can be contacted
- can the system which has been breached be shut down
- can the activity that led to the breach be stopped
- can access codes or passwords be revoked or changed
- did the data breach occur due to the actions of an external party (e.g. a cyber-attack)

Consideration will be given as to whether other processes or protocols outlined in QFD's policies or procedures should also be activated because of the data breach (i.e. cyber incident management).

QFD will take all measures when containing the data breach to not destroy information that may be needed to investigate the cause of the data breach.

6.3. Stage 3: Assessment

The types of personal information involved in the breach, in addition to other influencing factors, give rise to a varied range of potential harms to individuals that will need to be assessed on an individual basis.

As soon as practicable, QFD's RTI and Privacy Unit will assess the data breach to make a preliminary assessment of the risk posed by the breach. To undertake the assessment, QFD will gather as much information as possible regarding the data breach and determine the likelihood of serious harm, having regard to:

- the kind of personal information
- the sensitivity of the information
- is information protected by one or more security measures
- the likelihood the security measures could be overcome
- persons (or kinds), who have obtained, or who could obtain, the personal information
- the nature of the harm likely to result from the data breach
- depending on the circumstances, any other relevant matters, like how long information was exposed, circumstances of affected individual, how it occurred, combinations of personal information and actions taken by agency to reduce the risk of harm.

In addition to the information gathering process, QFD may also undertake a risk assessment for the assessment of serious harm.

During the assessment stage, QFD will take all reasonable steps to continue to contain the data breach.

All documentation gathered and created for the assessment process will be retained in accordance with QFD's records management procedures and in accordance with the *Public Records Act 2023*.

6.4. Stage 4: Notification

Unless an exemption applies, QFD's RTI and Privacy Unit will assist the Information Asset Custodian and/or the relevant business area where the data breach occurred in notifying affected individuals, the OIC and any other relevant parties of an eligible data breach. Other relevant parties may include:

- Minister for Local Government and Water and Minister for Fire, Disaster Recover and Volunteers
- Commissioner, QFD
- Queensland Policy Service
- Crime and Corruption Commission
- Queensland Government Chief Information Officer
- Office of the Australian Information Commissioner
- Australian Taxation Office
- Australian Cyber Security Centre
- any third-party organisations or agencies whose data may be affected
- financial service providers
- professional associations, unions or regulatory bodies.

Notification of an eligible breach to the OIC will include:

- whether QFD is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies
- the date the data breach occurred (if known)
- a description of the data breach, including the type of eligible data breach
- information about how the data breach occurred
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made
- the steps QFD has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach
- QFD's recommendations about the steps affected individuals should take in response to the data breach
- the number of individuals whose personal information was accessed, disclosed or lost and affected individuals for the data breach
- the total number of individuals notified of the data breach or, it is not reasonably practicable to work out the total number, an estimate of the total number
- whether the notified individuals have been advised how to make a privacy complaint to QFD.

Unless an exemption applies, as soon as practicable after forming a reasonable belief that a data breach is an eligible data breach, QFD will notify affected individuals:

- the contact details of QFD or a person nominated by QFD for further queries about the data breach
- the date the data breach occurred (if known)
- a description of the data breach
- information about how the data breach occurred
- QFD's recommendations about the steps an affected individual should take in response to the data breach
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made
- the steps QFD has taken to will take to contain the data breach and mitigate any harm caused to the affected individuals
- information about how an individual can make a formal privacy complaint.

Prior to providing notification, QFD is required to consider whether any of the exemptions detailed in Division 3 of Chapter 3A of the IP Act apply. Details of these exemptions are:

- investigations and proceedings (section 55)
- eligible data breach of more than one agency (section 56)
- agency has taken remedial action (section 57)
- inconsistency with confidentiality provision (section 58)
- serious risk of harm to health or safety (section 59)
- compromise to cybersecurity (section 60).

The method of notification will be determined on a case-by-case basis. Where QFD is unable to notify all affected individuals, alternative communication will be considered, such as a public notification on its website.

Notification is not mandatory for breaches outside the scope of an eligible data breach. However, QFD considers reasonable expectations of the individuals concerned when deciding to notify in these instances.

Tax file numbers – although the federal *Privacy Act 1988* (Cth) does not apply to QFD, any data breach involving tax file numbers must be handled in accordance with the mandatory notifiable data breach scheme under the federal Act. This includes notification to the affective individuals and to the Australian Office of the Information Commissioner.

6.5. Stage 5: Post-data breach review and remediation

After a data breach has been dealt with, a post breach review may be conducted on:

- the root cause of the data breach
- assets/controls impacted, and identification of improvements for the environment
- monitoring systems to identify areas for uplift revision
- relevant policies and procedures to reflect the lessons learned from the review
- service delivery practices that were involved in the breach.

All documents recording the review and remediation process, including action items identified, are to be retained in accordance with QFD's records management procedures and in accordance with the *Public Records Act 2023*.

7. Register of eligible data breaches

Section 72 of the IP Act requires QFD to establish and maintain an internal register of all eligible data breaches. The register must include specific information as prescribed in section 72 of the IP Act, such as:

- A description of the eligible data breach, including the type of data breach under section 47
- If the agency relied on an exemption, which exemption is relied on
- If a statement is required for the eligible data breach under section 51, the date the statement is provided
- If further information about the eligible data breach is required to be given to the Information Commissioner under section 52, each date the further information is given
- If individuals are notified under the eligible data breach under section 53(1)(a) or (b), the individuals notified and the date and method used to notify the individuals
- Details of the steps taken by the agency to:
  - Contain the eligible data breach; and
  - Mitigate the harm caused by the eligible data breach
- Details of the actions taken by the agency to prevent future data breaches of a similar kind occurring.

8. Recordkeeping

All actions taken in managing and responding to an actual data breach or a suspected data breach, including an eligible data breach, needs to be documented appropriately and provided to the relevant officers within QFD.

All documents created for the purposes of dealing with an actual data breach or suspected data breach, including an eligible data breach, are required to be retained by QFD in accordance with QFD's records management procedures and in accordance with the *Public Records Act 2023*.

9. Appendices

- Appendix A – Definitions

10. References

- *Information Privacy Act 2009* (Qld)
- P4.3 – Information Asset Management
- P4.6 – Queensland Privacy Principles – Privacy Policy
- PR4012 - Data Breach Response Plan (under development)
- Information Asset Custodian Delegation of Responsibilities

11. Implementation and review

This policy takes effect from 1 July 2025 and will be reviewed every three years to ensure it meets business needs and best practice guidelines.

Information used to inform the review may include:

- feedback received from customers, stakeholders and staff
- the results of internal or external reviews, audits or evaluations

- any changes in policy, legislation or organisational structure

12. Contacts

For further information regarding QFD's privacy requirements and obligations, please contact the QFD Right to Information and Privacy Unit via email to QFD.RTI@fire.qld.gov.au

Appendix A – Definitions

For the purposes of this policy, the following definitions apply:

Term	Definition
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act.
Australian Information Commissioner	The Australian Information Commissioner
Commonwealth Privacy Act	The *Privacy Act 1988* (Cth)
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 (section 47 of the IP Act).
Data Breach Policy	This policy.
Data Breach Response Plan	A more detailed procedural document complementing this data breach policy, which is an internal document detailing QFD's specific processes in managing and responding to a data breach.
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 QFD, **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 a loss of **personal information** held by QFD that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, **and** the loss likely to result in **serious harm** to any of the **individuals** to whom the information relates.
OIC	The Office of the Information Commissioner Queensland
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	Personal information means 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 (section 12 of the IP Act).
QFD employee	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: • an employee • a contractor or subcontractor or • an employee of a contractor or subcontractor • an apprentice or trainee • student gaining work experience • a volunteer

Sensitive information	Schedule 5 of the IP Act defines sensitive information as: Sensitive information for an individual, means the following— (a) Information or an opinion, that is also personal information, about the individual's— (i.) Racial or ethnic origin; or (ii.) Political opinions; or (iii.) Membership of a political association; or (iv.) Religious beliefs or affiliations; or (v.) Philosophical beliefs; or (vi.) Membership of a professional or trade association; or (vii.) Membership of a trade union; or (viii.) Sexual orientation or practices; or (ix.) Criminal record; (b) Health information about the individual; (c) Genetic information about the individual; (d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) Biometric templates.
Serious harm	Schedule 5 of the IP Act defines serious harm as: 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.
Tax file number	A tax file number (TFN) is a unique identifier issued by the Commissioner of Taxation to individuals and entities for tax administration purposes.