QIMR Berghofer	Data Breach Policy	Effective: 12 June 2025
		Version: 1.0
		Authorised by: CIO
		Approved by: Director & CEO

Contents

1 INTRODUCTION

This policy provides an overview of the Institute's procedures in relation to detecting, responding to, managing, notifying and reporting eligible data breaches in accordance with the Mandatory Notification of Data Breach Schedule (the MNDB Scheme), which is a requirement under Chapter 3A of the *Information Privacy Act 2009* (Qld) (IP Act).

2 PURPOSE AND SCOPE

2.1 Purpose

The purpose of this policy is to enable QIMR Berghofer to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals. It sets out the Institute's procedures for responding to data breaches, including its processes for meeting its assessment, notification and recording obligations when responding to a data breach.

2.2 Scope

This Policy applies to all Personnel (all Institute employees whether full-time, part-time or casual), volunteers, Council Members, Committee Members, students, Visiting Scientists, Honorary Scientists and Emeritus Scientists.

3 DATA BREACH

A 'Data Breach' means either of the following in relation to information held by the Institute:

a) unauthorised access to, or unauthorised disclosure of, the information; or
b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

The above definition encompasses any information held by the Institute.

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.

Examples of Data Breaches may include (but are not limited to):

- Unauthorised access to Personal Information by a third party (e.g., hacking or insider threats).
- Cyberattacks, such as phishing, ransomware, or malware incidents.
- Accidental disclosure, such as Personal Information being uploaded to a public website or shared with unintended recipients (e.g., sending an email to the wrong address).
- Loss or theft of devices containing Personal Information, such as laptops, USB drives, or mobile phones.

Data Breaches can be caused by or exacerbated by a variety of factors, affect different types of Personal Information, and give rise to a range of actual or potential harms to individuals, the Institute or other organisations.

4 NOTIFIABLE DATA BREACH

Not all data breaches require notification. In accordance with Queensland's mandatory data breach notification scheme, when QIMR Berghofer knows or reasonably suspects that a data breach is an eligible data breach, it will immediately and continue to take all reasonable steps to contain the data breach and mitigate the harm caused by the data breach. QIMR Berghofer will then as soon as practicable, notify the Information Commissioner and affected individuals.

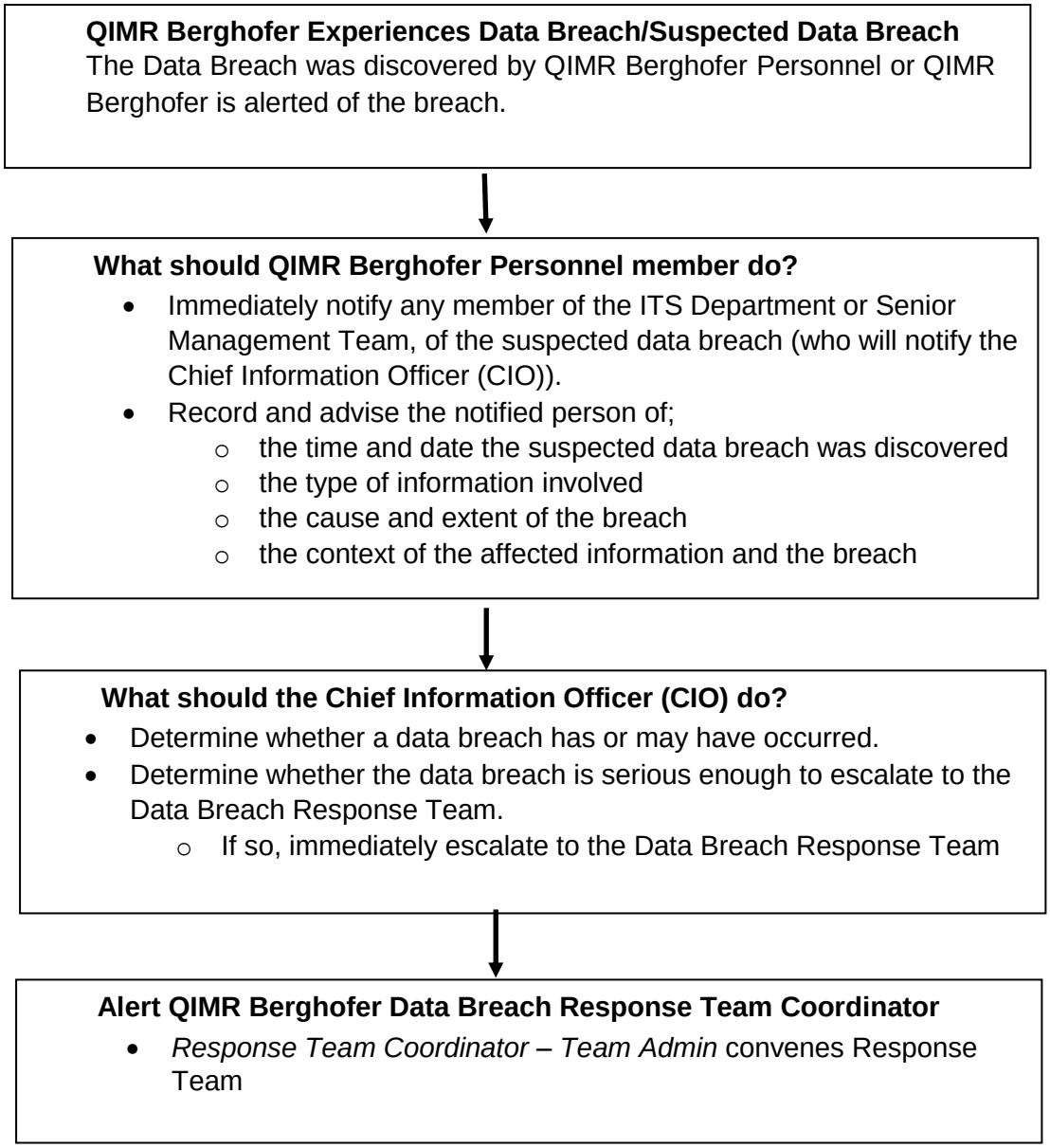
An eligible data breach occurs when there is unauthorised access to, loss of, or disclosure of Personal Information held by the Institute and the unauthorised access to or disclosure of the information is likely to result in serious harm to an individual to whom the Personal Information relates (e.g., physical, psychological, emotional, financial, or reputational harm).

In determining whether the Data Breach is likely to result in serious harm to an individual, the Institute will have regard to:

a) the kind of Personal Information accessed, disclosed or lost;
b) the sensitivity of the Personal Information;
c) whether the Personal Information is protected by 1 or more security measures;
d) if the Personal Information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome;
e) the persons, or the kinds of persons, who have obtained, or who could obtain, the Personal Information;
f) the nature of the harm likely to result from the Data Breach; and
g) any other relevant matter.

5 ASSESSING SUSPECTED DATA BREACHES

If any QIMR Berghofer Personnel suspects or becomes aware of a data breach, the Data Breach Response Plan is activated and must be followed. The plan requires a reasonable and expeditious assessment to determine if the data breach is an eligible data breach. The following chart outlines the staff roles involved in assessing a data breach.



When should the Chief Information Officer (CIO) escalate a data breach to the QIMR Berghofer Data Breach Response Team?

Chief Information Officer (CIO) to convene the response team when a data breach is suspected or confirmed, particularly if the breach involves sensitive Personal Information, has potential to cause serious harm, or requires immediate containment and investigation.

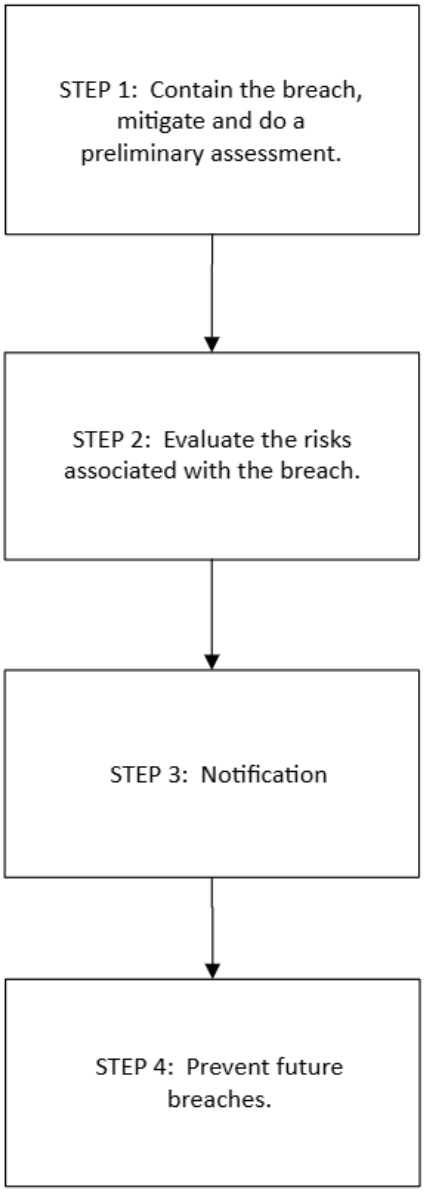
While not all breaches are equal—some may be minor and manageable without escalation—forming a Response Team ensures coordinated action for breaches with significant risks or complexities. The decision should be guided by the severity, scope, and potential impact of the breach on individuals and the Institute.

6 DATA BREACH RESPONSE TEAM ROLES AND RESPONSIBILITIES

The composition of the Data Breach Response Team and its roles and responsibilities are set out in the Business Continuity and Incident Management Procedure and the Data Breach Response Plan.

7 DATA BREACH RESPONSE

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.



7.1 Notifying the Office of the Information Commissioner (OIC)

If there is uncertainty as to whether the data breach is eligible, the Chief Operating Officer will assess whether there are reasonable grounds to believe the data breach is an eligible data breach within 30 days.

In the event that the Chief Operating Officer decides there has been an eligible data breach, it will be reported in line with the OIC IPOLA Guideline as soon as practicable.

7.2 Notifying the Individuals Affected

As soon as reasonably practicable after QIMR Berghofer has submitted the statement to the OIC, QIMR Berghofer: will notify individuals based on the OIC guidelines using one of the options outlined below, depending on what is reasonably practicable in the circumstances:

Option 1: Notify each individual;

Option 2: Notify each affected individual, if not reasonably practicable to notify each individual; or;

Option 3: Publish required information.

7.3 Records Management

Documents created by the Response Team will be saved in the Institute's corporate records management system.

8 ELIGIBLE DATA BREACH REGISTER

The Institute will maintain a register of all Eligible Data Breaches in line with OIC guidelines.

9 POST-BREACH REVIEW AND EVALUATION

Understanding what processes worked well, how issues were handled, and areas for improvement in the management of a data breach is an important component of the data breach administration process. This is particularly relevant to mitigating future risks, preventing reoccurrence or similar breaches, and improving Personal Information handling processes in line with expectations of the community and regulators.

The Data Breach Response Team will review all assessed Eligible Data Breaches, to:

- identify any lessons learnt and consider any short or long-term measures which could be taken to prevent the reoccurrence of a similar breach in the future.
- identify and remediate any improvements needed to process or procedures to enable the Institute to proactively and effectively manage data breaches.
- conduct a post-response assessment of how the Institute responded to the breach and the effectiveness of its Data Breach Response Plan.

10 ROLES AND RESPONSIBILITIES

All Personnel are responsible for identifying and reporting actual or suspected Data Breaches in accordance with this Policy.

11 MONITORING AND REVIEW

The Chief Information Officer is responsible for implementing and monitoring compliance with this policy.

This policy will be reviewed after one year, and then every three years.

12 DEFINITIONS

Refer to Delegations Framework/ Council Delegations for additional approved definitions.

Council	The Council of the Queensland Institute of Medical Research constituted under the QIMR Act.
Personnel	All QIMR Berghofer employees whether full-time, part-time, or casual, volunteers, Council Members, Committee Members, students, Visiting Scientists, Honorary Scientists and Emeritus Scientists
Institute	The Council of the Queensland Institute of Medical Research.
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.

13 RELATED DOCUMENTS

Information Privacy Act 2009 (Qld)

Privacy Act 1988 (Cth)

IPOLA Guideline MNDB Mandatory Notifications of Data Breach

IPOLA Mandatory Notification of Data Breach scheme – Exemptions

QIMR Berghofer Data Breach Response Plan

QIMR Berghofer Business Continuity and Incident Management Procedure

QIMR Berghofer Risk Management Procedure

14 CONTACT OFFICER

Chief Information Officer

15 AMENDMENT HISTORY

Version	Date approved	Approved by/Scope of change	Date due for review
1.0	12 June 2025	New Policy approved by Director & CEO	12 June 2028