PLAN
DATA BREACH RESPONSE POLICY AND PROCEDURE

Published:

JUNE 2024

CONTENTS

DOCUMENT INFORMATION

Version history

Document review date is as per the Integrated Management System Standard (HW2013-421/22.002).

This plan shall be reviewed and updated biannually or more often as necessary to ensure relevant and compliance to the PPIP Act.

Version	Author	Changes	Approved By	Date Approved
1	Carly Reid-Small	First Initial Release in response to changes to the NSW Legislation in 2023 which include the MNDB scheme.	Cheryl Eube – Group Manager Legal	21/06/24

Document control

Document Owner	Legal Counsel & Privacy Officer	Mandatory Reviewer(s)	Legal Team, General Counsel & Company Secretary
Approved By	Managing Director	TRIM No	HW2021-606/74.001
Approved Date	21/06/2024	Version No	1

1 Introduction

Hunter Water Corporation ('Hunter Water') has prepared and published this Data Breach Policy and Procedure ('DBPP') in accordance with the requirements of the Mandatory Notification Data Breach ('MNDB') Scheme detailed in Part 6A of the *Privacy and Personal Information Protection Act 1998 ('*PPIP Act*') (NSW).*

Hunter Water is committed to preventing and responding to data breaches in accordance with the requirements of the PPIP Act. Hunter Water acknowledges the value of personal information and its responsibility to ensure it is managed. The Privacy Framework has been developed to support all of Hunter Water's people to contribute to a privacy positive culture.

The Privacy Framework consists of the following:

- The Privacy Policy
- The Privacy Management Plan
- The Privacy Fact Sheet and
- This DBPP

This DBPP forms part of the overarching Hunter Water Corporate Emergency Response Plan ('CERP'). The CERP details the organisation and management of resources for dealing with all aspects of emergency management. Specifically, the DBPP details how Hunter Water will manage and respond to data breaches to ensure effective management of personal information and to fulfill legislative requirements.

This DBPP aligns with Hunter Water's value of trust. Hunter Water recognises that our people, customers, stakeholders and community trust us to keep their personal information safe and secure. We respect this trust and work together to continually improve the way that we respond to privacy and security threats.

2 Scope

This DBPP sets out Hunter Water's approach to complying with the MNDB Scheme, roles and responsibilities for reporting data breaches, and strategies for containing, assessing and managing eligible data breaches.

This DBPP applies to all of Hunter Water's people (as defined) and to all third-party providers or contractors who hold personal information or health information on behalf of Hunter Water.

3 Purpose

The purpose of this DBPP is to provide guidance to Hunter Water's people on preventing and responding to data breaches of Hunter Water held data, in accordance with the PPIP Act.

This DBPP sets out actions for managing an MNDB, including requirements around notifying persons where privacy may be affected by the breach.

This DBPP details:

- What constitutes an EDB under the PPIP Act
- Roles and responsibilities for reporting, reviewing and managing data breaches
- The steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent further data breaches

4 DELEGATION

Under Section 59ZJ of the PPIP Act the Managing Director delegates functions in the DBPP to the Data Breach Response Team.

The Data Breach Response Team (DBRT), will be comprised of the following roles:

- The General Counsel or Group Manager Legal
- Legal Counsel and Privacy Officer
- Group Manager Digital Services and Tech or Team Leader Information Security
- Group Manager Communications and Engagement
- Business Continuity Manager

For the purposes of this instrument, 'function' includes powers, authorities and duties, and anything ancillary or related to the exercise or performance of that function, but does not include the functions under the Act which require the Managing Director to form an opinion about a matter or make a decision.

5 Definitions, Acronyms and Abbreviations

Term or Phrase	Definition
Eligible Data Breach (EDB)	Defined in section 59D of the PPIP Act as: a. unauthorised access or disclosure of personal information held by Hunter Water that a reasonable person in the position of the Hunter Water would conclude is more likely than not to result in serious harm to the individual whose personal information has been compromised; or personal information has been lost in circumstances where unauthorised access or disclosure is more likely than not to occur and a reasonable person in the position of the Hunter Water would conclude is more likely than not to result in serious harm to the individual whose personal information has been lost.
Notifiable Data Breach (NDB)	A EDB that has either: ▪ occurred; or ▪ there are reasonable grounds to suspect that it might have occurred.
Assessor(s) and Assessment	The formal person(s) and investigation process under the Act who must be appointed and that must be conducted respectively.
Held	Information/data in the care and custody of Hunter Water or by an authorised third party on behalf of Hunter Water.
Health Information	As defined in section 6 of the *Health Records and Information Protection Act 2002* (NSW)
Hunter Water's people	Any individual employed by Hunter Water on a permanent, temporary or casual basis and all individuals performing work in any capacity for Hunter Water, such as contractors, subcontractors, agents, consultants, and those undertaking work experience, secondment and volunteer work.

Term or Phrase	Definition
Personal Information	As defined in section 4 of the PPIP Act. In this document, 'Personal Information' includes Health Information. Under section 4.1 of the PPIP Act personal information is broadly defined as, information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
Cyber Security Incident	As defined in section 12M of the *Security of Critical Infrastructure Act 2018 (Cth)* (SOCI Act): A cyber security incident is one or more acts, events or circumstances involving any of the following: a. unauthorised access to: i. computer data, or ii. a computer program b. unauthorised modification of: i. computer data, or ii. a computer program c. unauthorised impairment of electronic communication to or from a computer d. unauthorised impairment of the availability, reliability, security, or operation of: i. a computer, or ii. computer data, or iii. a computer program

6 Roles and Responsibilities

The following of Hunter Water's people have identified roles under this DBPP:

Role(s)	Responsibilities
Managing Director	Hunter Water's Managing Director will: ▪ Formally execute the delegations of functions to the Data Breach Response Team. ▪ Cause the actions mandated by section 59E(2) of the PPIP Act to take place. ▪ On receipt of notification of an actual or suspected EDB: o Immediately cause of reasonable steps to be taken to contain the data breach; and o Within 30 days and in an expeditious manner, cause to be carried out an assessment of whether the breach is, or there are reasonable grounds to believe the breach is an EDB ▪ Receive all reports in relation to data breaches and form an opinion and make all decisions mandated by the PPIP Act. ▪ Make all notifications to affected persons, and to the Privacy Commissioner, in relation to an EDB, as required under the PPIP Act.
Data Breach Response Team (DBRT)	The DBRT is instructed by and reports to the Managing Director. The DBRT and its members are responsible for carrying out any function under the PPIP Act delegated to it/them by the Managing Director.
People and Culture Team	The Learning and Development Team in collaboration with the Legal and Privacy Team is responsible for ensuring all of Hunter Water's people are made aware of, and provided adequate training in, their obligations under this DBPP.
Legal and Privacy Team	The Legal and Privacy Team is responsible for implementing this DBPP and ensuring that it is reviewed and updated in accordance with the requirements of this DBPP.
All Hunter Water's people (as defined)	All of Hunter Water's people are responsible for immediately reporting actual or suspected data breaches in accordance with this DBPP.

7 What is an 'Eligible Data Breach?'

An 'eligible data breach' ('EDB') is (as set out in section 59D of the PPIP Act):

- Unauthorised access to or disclosure of, personal information held by Hunter Water and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates; or
- Personal information held by Hunter Water is lost in circumstances where:
- Unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- If the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

8 How Hunter Water Has Prepared for a Data Breach

In preparation for the commencement of the PPIP Act, Hunter Water has taken a Privacy By Design approach which embeds privacy management into Hunter Water's operations through people, processes and systems.

The DBPP forms part of the Privacy Framework and has been prepared in the context of Hunter Water's related plans and processes to ensure a comprehensive approach to managing data breaches. Specifically, this DBPP is supported by:

- The Cyber Breach Response Plan
- The Corporate Emergency Response Plan
- External Communication and media reporting
- Procurement processes and provisions in contracts
- Ongoing privacy training and awareness schedules

8.1 Reporting and Responding to a Data Breach

There are five key steps required in the immediate response to a data breach or suspected data breach. In accordance with s 59E(2) of the PPIP Act, the Managing Director must:

1. Contain the breach
2. Assess the breach
3. Report the breach to the Privacy Commissioner
4. Notify affected persons
5. Undertake ongoing review and reporting

8.2 Contain the Breach

Immediately upon becoming aware that an EDB has occurred, or that there are reasonable grounds to suspect that an EDB might have occurred, Hunter Water's People must report the EDB (or suspected EDB) to the Managing Director.

The Managing Director must direct the DBRT to take or arrange all necessary possible steps to contain the breach and minimise any resulting damage (for example, shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords).

If a third party is in possession of the data and declines to return it, the Managing Director may direct the DBRT to obtain legal or other advice.

8.3 Assess the Breach

On receipt of the notification, the Managing Director must direct the DBRT to, and the DBRT must:

- immediately make all reasonable efforts to contain the data breach
- Within 30 days:
  - carry out an assessment as to whether the breach is, or there are reasonable grounds to believe the breach is, an EDB; and
  - take all reasonable steps to mitigate the harm caused by the EDB or suspected EDB throughout the assessment.

Extension of the Assessment

If the Managing Director is not satisfied that it is possible to conduct the assessment within 30 days:

- The Managing Director must, within that time frame, direct the DBRT to, and the DBRT must, start the assessment; and
- The Managing Director must give notice to the Privacy Commissioner that the assessment has begun; that an extension has been approved; and specify the new assessment period.

If the assessment is not concluded in the extended period the Managing Director must give written notice to the Privacy Commissioner that the assessment is ongoing; a new extension has been approved; and specify the new extension period.

Carrying Out the Assessment

The DBRT is to consider the following factors in carrying out the assessment:

- The type of personal information involved in the breach;
- The sensitivity of the personal information involved in the breach;
- Whether the personal information is or was protected by security measures;
- The persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given;
- The likelihood the persons specified in paragraph (d) above:
  - Have or had any intention of causing harm; or
  - Could or did circumvent security measures protecting the information
- The nature of the harm that has occurred or may occur; and
- Any other matter set out in any Privacy Commissioner guidelines.

Following the assessment, the DBRT must advise the Managing Director whether the data breach is an EDB, or there are reasonable grounds for believing that the data breach is an EDB.

8.4 Report the breach to the Privacy Commissioner

If, following the assessment, the Managing Director believes there has been an EDB, or there are reasonable grounds to believe there has been an EDB, the Managing Director must immediately notify the Privacy Commissioner of the EDB.

The notification to the Privacy Commissioner is to be made by way of approved form published by the Privacy Commissioner, and to address the following:

- The date the breach occurred;
- A description of the breach;
- How the breach occurred;

- The type of breach that occurred (e.g. unauthorised disclosure, unauthorised access, or loss of information);
- The personal information that was the subject of the breach;
- The length of time the personal information was disclosed;
- Actions taken or planned to be taken to secure personal information or to control or mitigate the harm done;
- Recommendations about what steps any individual affected should take in response to the EDB;
- Information about the making of privacy related complaints and internal review processes;
- The name of the agency the subject of the breach;
- Where other agencies may be involved, the names of the other agencies (and whether Hunter Water is reporting on behalf of those other agencies, and if so those agencies details);
- Whether the breach is a "cyber incident" – which is not defined in the PIPP Act but reliance is placed on the definition of a 'cyber security incident' under the SoCI Act as defined in section 4 of this DBPP;
- Contact details for the agency and a nominated contact person;
- The estimated cost of the EDB;
- The total, or estimated total, number of affected, or likely affected individuals, and:
  - the number notified of the EDB; and
  - the number informed about compliant and internal review procedures.

8.5 Notify affected persons

As soon as practicable after an EDB has occurred, the Managing Director must direct the DBRT to, and the DBRT must, take reasonable steps to notify each individual to whom the compromised personal information relates.

That notification must include the following details:

- The date the breach occurred;
- A description of the breach;
- How the breach occurred;
- The type of breach
- The personal information that was the subject of the breach;
- The length of time the personal information was disclosed;
- Actions
- Recommendations
- Information
- The name of the agency the subject of the breach;
- Where
- Contact details for the agency and a nominated contact person.

A template Correspondence to Affected Individuals or Organisations is provided at Appendix 1 to this DBPP.

If the DBRT cannot reasonably carry out all such notifications, the Managing Director must direct the DBRT to, and the DBRT must, publish a notification on the public notification register to be kept by Hunter Water on its website details of the EDB and:

- include the information required to be notified to affected individuals or organisations (as set out above), for at least 12 months after the date the notification is published;
- except to the extent that it contains personal information or would prejudice Hunter Water's functions;

As soon as practicable after the notification is published on the website the Managing Director must notify the Privacy Commissioner about how to access the notification on the public notification register (eg by providing a link).

8.6 Ongoing review and reporting

Pursuant to s 59Q of the PPIP Act, the Managing Director will continue to review the EDB and will notify the Privacy Commissioner of any new information, or if any exemption (detailed in clause 12 hereof) is determined to apply to Hunter Water.

9 Exemptions

9.1 Involvement of Multiple Agencies

If the EDB involves multiple agencies, once each agency has notified the Privacy Commissioner of an EDB, all heads or chief executive officers (as the case may be) need not embark further notifications if the head of one agency undertakes to do the notifications for all the affected agencies.

9.2 Prejudice to Proceedings

The Managing Director does not have to carry out the notifications to individuals or public notifications if they reasonably believe such notification would be likely to prejudice:

- Investigations that may lead to prosecutions;
- Proceedings in a Court or Tribunal; or
- Any matter prescribed in the regulations.

9.3 Mitigation has been effective

If mitigating steps have been taken:

- In the case of unauthorised access to personal information, if the mitigating action is taken before the unauthorised access results in serious harm to an individual, and because of the mitigation action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to an individual; or
- In the case of loss of personal information, if the mitigating action is taken before there is unauthorised access or disclosure, and there is in fact no unauthorised access or disclosure because of the mitigating action taken;

then the Managing Director does not have to carry out the notifications to individuals or public notifications.

9.4 Secrecy

If notifications are inconsistent with a secrecy provision of any Act or statutory rule then the Managing Director is exempt from notifications to individuals or public notifications requirements.

9.5 Serious Risk of harm to health and safety

If the Managing Director reasonably believes that notification would create a serious risk of harm to an individual's health or safety then the Managing Director may exempt HWC from notifications to individuals or public notifications requirements.

In making the decision the Managing Director must:

- consider the extent to which the harm of notification is greater than the harm of not notifying;
- consider the currency of the information relied upon in ascertaining the serious risk of harm to an individual; and
- not use and access other personal information held by HWC to assess the impact of notification, unless the Managing Director knows or reasonably believes there is information relevant to whether an exemption should be given.

The Managing Director must have regard to the guidelines prepared by the Privacy Commissioner in making a decision to exempt HWC under this section.

The exemption may be permanent, or for a specific period, or until the happening of a particular thing.

The Managing Director must, by written notice to the Privacy Commissioner, notify the Privacy Commissioner that the exemption is relied on; the details about whether the exemption is permanent or temporary; and if the exemption is temporary, of the specified or expected time the exemption is to be relied upon.

9.6 Exemptions to prevent compromising cyber security

If the Managing Director reasonably believes that notification would worsen HWC's cyber security or lead to further data breaches then the Managing Director may exempt HWC from notifications to individuals or public notifications requirements, but only for as long as is necessary to prevent the situation worsening or further data breaches occur.

In making the decision the Managing Director must consider guidelines issued by the Privacy Commissioner and must give written notice to the Privacy Commissioner:

- That an exemption under s 59X is relied on;
- When the exemption is expected to end;
- The manner in which the exemption will be reviewed.

The Managing Director must review the exemption each month and provide an update to the Privacy Commissioner on the review of the exemption.

10 Prevention of Future Repeat Data Breaches

If an EDB occurs, Hunter Water will further investigate the circumstances of the breach to determine all causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include:

- A security audit of both physical and technical security controls;
- Review of policies and procedures;
- Review of staff/contractor training practices; and/or
- Review of contractual obligations with contracted third-party service providers.

11 Breaches of this DBPP

A breach of this Policy by any of Hunter Water's people, as a subset of the Code of Conduct, may result in disciplinary action up to and including termination of employment (consistent with the Performance Management, Misconduct and Disciplinary Policy). Contractors may be subject to contract renegotiation, including termination.

Any suspected breaches will be investigated in line with the Complaints and Allegations Policy.

12 Related Legislation, Policies and Guidance

Doc ID	Document Title
Act	Privacy and Personal Information Act 2009 (NSW)
Act	Government Information (Public Access) Act 1998 (NSW)
Act	Health Records and Information Privacy Act 2002 (NSW)
Policy	Privacy Policy (Hunter Water)
Plan	Privacy Management (Hunter Water)
Fact Sheet	Privacy (Hunter Water)

APPENDIX A: TEMPLATE CORRESPONDENCE TO AFFECTED INDIVIDUALS OR ORGANISATIONS

Dear [name]

I am writing on behalf of Hunter Water Corporation ('Hunter Water') with important information regarding a recent data breach involving your personal information. Hunter Water became aware of the breach on [date].

The breach occurred on or about [date] and the details are as follows:

[address:

- A description of the breach;
- How the breach occurred;
- The type of breach that occurred (e.g. unauthorised disclosure, unauthorised access, or loss of information)
- The personal information that was the subject of the breach;
- The length of time the personal information was disclosed;
- Actions taken or planned to be taken to secure personal information or to control or mitigate the harm done;
- Recommendations about what steps any individual affected should take in response to the EDB;
- Where other agencies may be involved, the names of the other agencies (and whether Hunter Water is reporting on behalf of those other agencies, and if so those agencies details)]

I am the nominated officer dealing with this matter. Please call me with any questions or concerns you may have about the data breach. My contact details are at the bottom of this letter.

We have established a section on Hunter Water's website [insert link] with updated information and links to resources that offer information about this data breach.

We take our role in safeguarding your data and using it in an appropriate manner seriously. Please be assured that we are doing everything we can to rectify the situation.

Please note that under the *Privacy and Personal Information Protection Act 1998* (NSW) you are entitled to register a complaint with the NSW Information and Privacy Commission with regard to this breach. Complaints may be forwarded to the following:

Office: Information & Privacy Commission

Level 11, 1 Castlereagh Street Sydney NSW 2000

Post: GPO Box 7011 Sydney NSW 2001

Phone: 1800 472 679 Fax: 02 8114 3756

Email: ipcinfo@ipc.nsw.gov.au **Website**: www.ipc.nsw.gov.au

Should you have any questions regarding this notice, or if you would like further information, please do not hesitate to contact me.