Data Breach Policy

Implementation officer	General Counsel & Company Secretary
Relevant to	The WaterNSW Board All WaterNSW Employees
Relevant documents	WaterNSW Code of Conduct WaterNSW Privacy Policy WaterNSW Privacy Management Plan WaterNSW Information Classification and Handling Standard March 2022 Information and Privacy Commissioner Guidelines on the assessment of data breaches under Part 6A of the PPIP Act September 2023
Relevant legal and other requirements	*Privacy and Personal Information Protection Act 1998* (NSW) *Health Records and Information Privacy Act 2002* (NSW) *Privacy Act 1988* (Cth) *Government Information (Public Access) Act 2009* (NSW) *State Records Act 1998* (NSW)

Monitoring, Evaluation and Review, Revision history

Outcome: How does this Plan deliver against the purpose and scope?	
Monitoring	This policy is subject to ongoing monitoring in order to reflect current practices within WaterNSW, and best practice guidelines.
Evaluation and Review	This document is risk rated as a Major level based on the WaterNSW Risk Management Rating table. It will be reviewed no later than every year unless a change in legislation or regulatory requirement commands the need to review.
Revision history	Document created December 2023.

Risk Rating	**Recommended Review Period**
Extreme	Annually
Major	Annually
Medium	2 years
Minor	3 years

Approval

Joe Pizzinga
Executive Manager Finance, Legal & Risk

Contents

1. PURPOSE AND SCOPE

This purpose of this Policy is to set out the WaterNSW procedures for responding to data breaches, including its processes for meeting its assessment, notification and recording obligations in relation to Eligible Data Breaches.

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) establishes the NSW Mandatory Notification of Data Breach Scheme (**MNDB Scheme**). The MNDB Scheme requires each organisation bound by the PPIP Act (including WaterNSW as a state owned corporation) to notify the Privacy Commissioner and affected individuals of Eligible Data Breaches.

This Policy applies to all WaterNSW Employees, and to all Personal and Health Information that is in the possession or control of WaterNSW or is contained in a State record in respect of which WaterNSW is responsible under the *State Records Act 1998* (NSW). Unless otherwise stated, a reference to "information" in this Policy is a reference to both Personal Information and Health Information.

This Policy supplements WaterNSW's Privacy Management Plan. More information about how WaterNSW collects, uses and discloses Personal and Health Information can be found within that Plan.

The MNDB Scheme imposes a number of obligations on the head of an agency (i.e. WaterNSW's Chief Executive Officer). Pursuant to s 59ZJ of the PPIP Act, those functions have been delegated to the General Counsel & Company Secretary.

2. WHAT IS AN ELIGIBLE DATA BREACH?

2.1 What is a data breach?

A data breach occurs when personal or health information held by an agency is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

Data breaches can occur as a result of malicious action, systems failure or human error or misconception. A data breach can still occur even if no information has been disclosed outside of WaterNSW (eg. unauthorised access to personal information by an Employee).

The following are examples of data breaches:

- accidental loss or theft of classified material data or equipment on which information is stored (e.g. loss of paper record, laptop, tablet or mobile phone, compact disk or USB stick)
- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain

unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of classified material or information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or information posted onto WaterNSW website without consent
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to WaterNSW information or information systems

2.2 What is an Eligible Data Breach?

The MNDB Scheme applies where an Eligible Data Breach has occurred. Not all data breaches will be Eligible Data Breaches. To constitute an Eligible Data Breach two tests must be satisfied:

1. there is:
    a. unauthorised access to information, or
    b. unauthorised disclosure of information, or
    c. likely to be unauthorised access to or unauthorised disclosure of information (a loss); ***and***
2. a reasonable person would conclude that the unauthorised access, unauthorised disclosure or loss would be likely to result in serious harm to an individual to whom the information relates.

An Eligible Data Breach may occur within WaterNSW, between WaterNSW and one or more public sector agencies, and where an external person or entity accesses data held by WaterNSW without authorisation.

3. SYSTEMS AND PROCESSES FOR MANAGING DATA BREACHES

WaterNSW has a range of systems and processes in place to prevent and manage data breaches. A number of cyber security measures are in place across WaterNSW's IT network and infrastructure to protect against data breaches. Further information about storage and security measures can be found within the WaterNSW Privacy Management Plan and the IT Information Security Policy.

WaterNSW will ensure all Employees and third-party providers who store personal and health information on behalf of WaterNSW are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches.

Additionally, WaterNSW's Board Committee on Audit & Risk monitors and evaluates privacy risk management activities within WaterNSW, and receives annual reports in relation to all reported known or suspected data breaches (whether minor or serious).

4. REPORTING AND RESPONDING TO AN ELIGIBLE DATA BREACH

There are five key steps in responding to an Eligible Data Breach. These steps should be carried out for all suspected Eligible Data Breaches to determine if the breach is an actual Eligible Data Breach for the purposes of the PPIP Act:

1. Internal notification
2. Containment
3. Assessment
4. External notification
5. Preventative action

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

4.1 Step 1: Internal notification

Employees

Where an actual or suspected Eligible Data Breach is discovered by an Employee, notification must be provided immediately to the General Counsel & Company Secretary. If an Employee is unsure whether a matter should be notified, the Privacy Contact Officer should be contacted immediately for further advice.

The notification must be via email and must include as much information as possible, including:

a. the date the breach occurred,
b. the date the Employee became aware of the breach,
c. a description of the breach,
d. how the breach occurred,
e. the type of breach that occurred,
f. the information that was the subject of the breach,
g. the amount of time the information was disclosed for, and
h. any actions that have been taken or that are planned to ensure the information is secure, or to control or mitigate any harm done to an individual.

Members of the public

Members of the public are also encouraged to report any known data breaches by or from WaterNSW to the Privacy Contact Officer:

Email: privacy@waternsw.com.au
Phone: 02 9865 2457

4.2 Step 2: Containment

Once a potential breach is notified, containing the breach is the immediate concern. All reasonable efforts must be taken to contain the breach and minimise any resulting damage.

Examples of measures to contain a breach include seeking to recover the information, shutting down the system that has been breached, suspending the activity that led to the breach, revoking access or changing access codes or passwords.

If a third party is in possession of the information and declines to return it, it may be necessary for WaterNSW to seek legal or other advice on what action can be taken to recover the information. When recovering information, WaterNSW will undertake reasonable efforts to make sure that copies have not been made by the third party or, if they have, that all copies are recovered.

4.3 Step 3: Assessment

The General Counsel & Company Secretary, or a person(s) directed by the General Counsel & Company Secretary (**Assessor**), must carry out an assessment of whether the breach is an Eligible Data Breach or there are reasonable grounds to believe the breach is an Eligible Data Breach (**Assessment**).

Any person who the General Counsel & Company Secretary reasonably suspects to be involved in any action or omission that led to the breach is not permitted to carry out the Assessment.

Factors for consideration in Assessment: As noted above (see section 2.2), a data breach will constitute an Eligible Data Breach where two tests are satisfied:

- accidental use, disclosure or loss of information, 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.

The term 'serious harm' is not defined within the PPIP Act. Harms that can arise from a data breach are context-specific and will vary based on a number of factors. However, serious harm will occur where the harm arising has, or may, result in a real or substantial detrimental effect to the individual; the effect on the individual must be more than mere irritation, annoyance or inconvenience.

The Privacy Commissioner has published Guidelines on the assessment of data breaches under Part 6A of the PPIP Act which must be considered by the Assessor.

In general, the Assessor should have regard to the following factors in undertaking the Assessment (this is not an exhaustive list):

a. The types of information involved in the breach (for example, some types of information may carry more inherent risk than others, such as financial or health information),
b. The sensitivity of the information involved in the breach (which may arise from the type of information alone, or from the fact that a combination of data has been compromised (eg. bank account information together with identity information) ,
c. Whether the information is or was protected by security measures,
d. The persons to whom the unauthorised access to, or unauthorised disclosure of, the information involved in the breach was, or could be, made or given,
e. The likelihood the persons specified in (d):
    i) Have or had the intention of causing harm, or
    ii) Could or did circumvent security measures protecting the information,
f. The nature of the harm that has occurred or may occur (eg. potential identity theft, financial loss, emotional distress or embarassment, reputational damage, loss of employment, physical harm,etc),
g. The extent to which affected individuals may be particularly vulnerable to harm, and
h. The ease with which information can be accessed and individuals identified.

Time to conduct the Assessment: The Assessment must be conducted in an expeditious way and the Assessor must take all reasonable steps to ensure the Assessment is completed within 30 days of the date that the Employee became aware of a breach (as advised in the internal notification of the breach set out at Step 1).

If the General Counsel & Company Secretary is satisfied that an Assessment cannot reasonably be conducted within 30 days, they may approve an extension of the time period to conduct the Assessment. Notification of the extension (and any further extensions given by the General Counsel & Company Secretary) will be required to be given to the Privacy Commissioner in accordance with s.59K of the PPIP Act.

Report on findings of Assessment: Following completion of the Assessment, the Assessor must provide a report to the General Counsel & Company Secretary as to whether the Assessment found that the breach is an Eligible Data Breach, or there are reasonable grounds to believe the breach is an Eligible Data Breach.

Decision on Assessment: The General Counsel & Company Secretary must then decide whether the breach is an Eligible Data Breach, or whether there are

reasonable grounds to believe the breach is an Eligible Data Breach. The Chief Executive Officer and the Executive Manager Finance Legal & Risk are to be briefed on the decision made following the assessment.

Mitigation of harm during Assessment: During the conduct of an Assessment, WaterNSW has a responsibility to make all reasonable attempts to mitigate the harm done by a suspected breach.

4.4 Step 4: External notification

If the breach is assessed to be an Eligible Data Breach (as a result of the assessment in Step 3), WaterNSW has a legal obligation under the PPIP Act to notify the Privacy Commissioner and affected individuals, unless an exemption applies. These notification requirements are discussed further below.

4.4.1 Notification to the Privacy Commissioner:

If a decision is made that a breach is an Eligible Data Breach, the General Counsel & Company Secretary must *immediately* (and in consultation with the Executive Manager Finance Legal & Risk) notify the Privacy Commissioner. The notification must be in the approved form (located on the NSW Information and Privacy Commission website).

The information requested by the approved form must be completed unless it is not reasonably practicable for the information to be provided.

Further notification to the Privacy Commissioner may be required under s.59Q of the PPIP Act.

4.4.2 Notification to affected individuals:

If a decision is made that a breach is an Eligible Data Breach, *as soon as practicable* and to the extent that it is reasonably practicable, the General Counsel & Company Secretary must take reasonable steps to notify affected individuals of the information set out in s.59O of the PPIP Act about the Eligible Data Breach. The Executive Manager Corporate Affairs should be consulted prior to notifications being issued to affected individuals.

If one of the exemptions set out in Pt.6 Div.4 of the PPIP Act applies in relation to an Eligible Data Breach, notification to affected individuals may not be required. The General Counsel & Company Secretary *must* be consulted for advice in relation to any applicable exemptions.

If affected individuals cannot be notified, or if it is not reasonably practicable to do so, WaterNSW must publish a notification of the breach in its public notification register (see further section 4.4.3 below).

4.4.3 Registers

WaterNSW will keep a record of any public notification of an eligible data breach on a Public Data Breach Register on its website, pursuant to s.59P of the PPIP Act. Reasonable steps must also be taken to publicise the notification, and the notification must remain published for at least 12 months.

The Privacy Commissioner must be informed of and provided with access to any notification on WaterNSW's public notification register. Information about how to access WaterNSW notifications will be published on the Privacy Commissioner's website for at least 12 months.

WaterNSW is also required to maintain an internal Eligible Data Breach Incident Register in accordance with s.59ZE of the PPIP Act.

4.5 Step 5: Preventative action

WaterNSW 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 or similar breach in the future.

Preventative actions could include:

- review of WaterNSW's IT systems and remedial actions to prevent future breaches,
- security audit of both physical and technical security controls,
- review of policies and procedures,
- review of staff/contractor training practices,
- review of contractual obligations with contracted service providers,
- any other actions deemed necessary by WaterNSW.

5. AUTHORITIES AND RESPONSIBILITIES

Role	Responsibility
WaterNSW Board	Has the authority and responsibility to: • Maintain an awareness and understanding of this Policy.
Audit and Risk Board Committee	Has the authority and responsibility to: • Review annual reports in relation to all reported known or suspected data breaches (whether minor or serious).
Chief Executive Officer	Has the authority and responsibility to: • Make all reasonable efforts to contain a data breach • Make all reasonable attempts to mitigate the harm done by a suspected breach

Executive Managers[17] and Direct Reports to Executive Managers	Have the authority and responsibility to: • Endorse and promote this Policy, including through ensuring Employees are aware of obligations to report suspected data breaches. • Support managers in implementing actions to contain data breaches and mitigate their impact.
Executive Manager Corporate Affairs	Has the authority and responsibility to: • In the case of a confirmed Eligible Data Breach, advise on the communication strategy and messaging to affected individuals.
General Counsel & Company Secretary	Has the authority and responsibility to (under delegation pursuant to s 59ZJ of the PPIP Act): • Receive reports of suspected data breaches. • Direct assessments of data breaches and approve extensions to assessment periods for data breaches. • Determine whether a data breach is an Eligible Data Breach. • Notify the Privacy Commissioner of matters required under the MNDB Scheme. • Consult with the Executive Manager Corporate Affairs in relation to the communication strategy to notify affected individuals of matters required under the MNDB Scheme. • Provide updates as required to the Chief Executive Officer and Executive Manager Finance Legal & Risk in relation to data breaches.
Employees	Have the authority and responsibility to: • Maintain an awareness of this Policy. • Immediately report all suspected data breaches in accordance with this Policy.

DEFINITIONS

Eligible data breach see section 2.2.

Employee means, for the purposes of this Policy, any person working as a direct employee of WaterNSW or in the capacity of a contractor or consultant whether in a casual, temporary, or permanent capacity.

Health Information means Personal Information that is information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person, see section 6 of the *Health Records and Information Protection Act 2002* (NSW).

MNDB Scheme means the mandatory data breach scheme set out in Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW).

Personal Information means 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, including such things as name, email address, mobile phone number or residential address. Health Information is excluded from the definition of Personal Information, except for the purposes of the MNDB Scheme. Other exclusions from Personal Information are also set out in section 4(3) of the PPIP Act.

PPIP Act means the *Privacy and Personal Information Protection Act 1998* (NSW).

Privacy Commissioner means the Privacy Commissioner appointed under the PPIP Act.