Policy

Data Breach Policy

1. Overview

1.1 At a glance

A Data Breach Policy is essential to ensure that Sydney Water responds quickly and confidently in the event that it, one of its contractors or third parties suffers an eligible data breach as defined under the *Privacy and Protection of Personal Information Act 1998* (NSW) (**PPIP Act**).

The policy outlines how Sydney Water is made aware of and will respond to an eligible data breach that it or its third parties suffers. This policy complies with section 59ZD of the PPIP Act.

1.2 Scope

This policy applies to:

- All employees and contractors
- All third party service providers
- All affected individuals whose personal and/or health information is held by Sydney Water
- All personal and health information collected, held or managed by Sydney Water.

1.3 Objective

The policy puts in place Sydney Water's plan to manage a data breach, so that it can:

- Identify, contain, assess and respond to a breach
- Have roles and responsibilities established to deal with a breach
- Report breaches to the appropriate bodies and individuals
- Minimise the harm caused to affected individuals (as defined in the PPIP Act) and restore trust in Sydney Water and the NSW Government.

2. Policy in detail

Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**) establishes the NSW Mandatory Notification of Data Breach (**MNDB**) scheme.

The MNDB scheme requires Sydney Water to notify the Privacy Commissioner and affected individuals of eligible data breaches.

Under the scheme, Sydney Water is required to prepare and publish a Data Breach Policy (**DBP**) for managing such breaches.

2.1 Our position on privacy

Sydney Water recognises that to deliver world class water services to its customers, it must carefully manage the personal and health information of our customers, employees and other members of the community.

We treat privacy seriously and have established a privacy framework to support this. We have prepared for a data breach by reviewing relevant policies and procedures and introducing a Data Breach Response Plan (**DBRP**). We assess high risk processes, programs, projects and decisions for privacy impacts and embed privacy into other frameworks, including the enterprise risk and incident management frameworks. This is supported by mandatory training for employees on how to handle data breaches and other privacy related matters. Further details of this can be found in our Privacy Management Plan (**PMP**).

We ensure our delivery partners and third parties are aware of our position on privacy and how to meet these obligations.

We test our framework to ensure that it works as intended and identify areas where we can enhance our privacy practices.

We take a 'no wrong doors' approach to privacy and encourage everyone to be privacy minded. If you suspect a data breach has occurred, please contact the Privacy Manager immediately at privacy@sydneywater.com.au.

2.2 What is a data breach

A data breach occurs when there is:

- Unauthorised access to, or
- Unauthorised disclosure of, or
- Loss or theft of

Personal and/or health information.

A data breach may be the result of a deliberate or accidental occurrence due to social engineering, hacking, misconfiguration of system controls or settings, loss or theft of devices, or inadvertent disclosures caused by human error.

2.2.1 Eligible data breaches

An eligible data breach occurs when the data breach is reasonably likely to cause serious harm to an individual or individuals affected.

The serious risk of harm could be:

- Financial loss or fraud
- Identity theft
- Damage to reputation
- Safety or violence.

An eligible data breach must be reported to the NSW Privacy Commissioner, affected individuals and in some circumstances the Australian Information Commissioner. The notification requirements can be found in Part 6A of the PPIP Act (also known as the MNDB scheme) and the *Privacy Act 1988* (with respect to the Notifiable Data Breach Scheme – Part IIIC).

Eligible data breaches may also need to be reported to other agencies and entities, such as Cyber NSW, Department of Customer Service, Australian Cyber Security Centre (ACSC), NSW Police, Australian Federal Police, our insurer, etc.

2.3 Strategies for identifying, containing, assessing and managing eligible data breaches

2.3.1 Identifying a breach

A suspected or actual data breach could be identified by a Sydney Water employee, contractor, business partner, other government agency or member of the public. This could occur because of an internal action (such as human error or self-discovered breach), or an external factor (malicious attack, report from a customer).

It is important that if you suspect a data breach that you report it immediately to the Privacy team at privacy@sydneywater.com.au for investigation.

Early identification of a data breach gives Sydney Water the best opportunity to contain the breach and limit the harm that may occur.

Our employees must follow the DBRP if they identify a data breach. If a data breach is identified in another incident management process, it will interface with our DBRP.

If you identify a suspected or actual breach, make sure you have attempted to gather the following information, at a minimum:

- the time and date the suspected breach was discovered,
- the type of personal information involved,
- the cause and extent of the breach, and
- the context of the affected information and the breach.

2.3.2 Contain and preliminary assess the breach

Being able to contain a breach could limit the risk of harm the breach causes. Depending on whether the data breach is due to human error or malicious attack, Sydney Water will attempt to contain the breach by:

- Contacting the recipient of the information if it was sent in error
- Preventing the breach from continuing
- Limiting or disabling access to the information

- Taking services offline
- Wiping devices
- Working with third party providers.

Any attempts to contain a breach should be documented and the results will be used to make a preliminary assessment of the breach.

2.3.3 Assessing the breach

Within the MNDB scheme, there are timeframes, certain steps and a responsibility to assess a data breach promptly. These activities are delegated from the Managing Director to the Privacy team.

The activity of assessing a data breach is to determine what happened/occurred and whether a serious risk of harm to an individual is more likely to occur than not. If it is more likely than not, it will meet the definition of an eligible data breach.

During this step, attempts to contain the breach, or mitigate the harm could be occurring.

We will rely on the guidance from the IPC to assess the harm and engage with internal and external stakeholders and subject matter experts to assess the breach.

In some circumstances, Sydney Water may rely on an extension to the 30 day assessment timeframe if we are unable to determine whether the breach meets the threshold test of serious risk of harm to an individual to whom the information subject to unauthorised access, unauthorised disclosure or loss relates. Eligible data breaches that meet this threshold test need to be communicated to the NSW Privacy Commissioner.

Preliminary decisions on the assessment will be provided to our Managing Director. If the breach is assessed as an eligible data breach, we will follow the requirements of the MNDB scheme and notify. If the threshold test of serious risk of harm to an individual is not met, we will continue to review and manage the breach.

2.3.4 Managing a breach

Irrespective of whether a data breach is an eligible data breach, Sydney Water will manage a data breach according to its incident management processes. The management of a data breach will ensure:

- Relevant stakeholders are involved in responding to the breach and making decisions in the best interest of affected individuals and Sydney Water
- Responsibility of specific tasks are assigned and followed through
- Decisions about when and how to assess/re-assess and notify are made clear.

The Privacy Manager will ensure records of the identification, containment and assessment of data breaches are made and kept by Sydney Water in accordance with its record keeping obligations.

2.3.5 Notification of an eligible data breach

Sydney Water will notify the NSW Privacy Commissioner immediately of any eligible data breaches using the approved form made available on the Information and Privacy Commission (**IPC**) website. Sydney Water may also notify other law enforcement and government agencies of a breach if required to do so.

Sydney Water will also notify individuals affected by a data breach as soon as practicable, unless we have reason to exercise an exemption from doing so. Notification will occur directly with the individual in the first

instance. However, if we are unable to directly notify individuals, we will publish a notification of the data breach on our website and publicise this.

We will follow and apply the requirements of the MNDB scheme, including what information to provide when notifying the Privacy Commissioner and affected individuals.

In some circumstances, Sydney Water may choose to notify media outlets to ensure that affected individuals are made aware of the data breach.

Sydney Water will also publish its Public Notification Register on its website when Sydney Water chooses to notify affected individuals publicly rather than individually if it is impracticable to notify such individuals personally.

2.4 Responding to a breach

Sydney Water's response to a breach will depend on the nature of the breach. At a minimum, Sydney Water will have:

- a dedicated officer to invoke the data breach response plan
- a data breach response team to assist with the response to a breach
- a communication strategy to keep those affected informed
- external expertise available upon request or need.

Sydney Water employees including contractors should consult the Sydney Water DBRP for further information on how to respond to a data breach. The plan is available on Sydney Water's intranet and details specific procedures to follow in the event of a data breach.

2.4.1 Communication strategy

Sydney Water's Privacy Manager will work with the Communications Teams when issuing communications under this policy. Sydney Water will aim to provide information about an eligible data breach to external bodies including law enforcement or government agencies, and the relevant affected individuals within five business days. Our website will contain a link to this policy as well as to the Public Notification Register, where applicable.

2.5 Roles and responsibilities

2.5.1 Sydney Water roles

Sydney Water has identified key roles within the organisation that will assist it with a data breach. The roles include members of the Legal, Communications, IT, Risk, Insurance, Security, Customer Services and People and Culture functions and teams.

2.5.2 Third parties

We will work with third parties to establish a clear understanding of a data breach that they suffer and report to us.

If you are a third party provider of Sydney Water and you suspect or suffer a breach that may affect Sydney Water, immediately contact the Privacy Manager at privacy@sydneywater.com.au .

2.5.3 Subject matter expertise

Sydney Water will utilise subject matter expertise as required. This may include forensic specialists, other government agencies, law enforcement agencies and identity fraud hyper-care services.

2.6 Testing the policy

Sydney Water takes its role of protecting personal information seriously. We will test and review the policy on a continuing basis to ensure it is fit for purpose and evolves over time.

2.7 Recordkeeping

Sydney Water will document information of any data breaches it is notified about as part of its obligations under the MNDB scheme and the *State Records Act 1998*.
Sydney Water will maintain the following registers:

- Public Notification Register
- Sydney Water Internal Register of Data Breaches

2.8 Post Breach Review and Evaluation

Sydney Water will undertake a review into the circumstances of a data breach to determine relevant causes that may have contributed to the breach occurring after the breach has occurred. Any learnings to prevent or mitigate future data breaches will be identified and shared internally.

Over time, we will also review our breach response records to identify trends and weaknesses to remedy.

2.9 Staff Training and Awareness

Sydney Water requires online learning modules on privacy and other topics must be completed by all existing and new employees. We also run targeted sessions and training within the organisation and use events such as Privacy Awareness Week and Cyber Awareness Month to profile and raise awareness of privacy and data breaches.

3. Definitions

Term	Definition	Source
Data breach	Refer to section 2.2	PPIP Act
Eligible data breach	Refer to section 2.2	PPIP and Privacy Acts
Personal information	Information or an opinion about an identifiable individual	PPIP Act
Health information	Personal information about an individual's physical or mental health or disability, health services provided or to be provided	HRIP Act