Sydney Metro Data Breach Policy

SM-23-00905652

1 Purpose of the policy

This policy prescribes the principles and requirements that must be applied by all Sydney Metro staff to meet our obligations under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) in the event of a suspected or actual eligible data breach.

In the event of a privacy or data breach, the Sydney Metro Privacy Data Breach Response Procedure sets out how to manage and respond to the breach.

Sydney Metro is committed to protecting the privacy of our customers and staff through the appropriate collection and handling of personal and health information in accordance with the Sydney Metro Privacy Management Plan.

Sydney Metro is required to prepare and publish this policy under section 59ZD of the PPIP Act. For the purposes of this policy, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002* (HRIP Act).

2 Who is this policy for?

This Policy applies to permanent, temporary and casual staff, staff seconded from another organisation, and contingent workers including labour hire, professional services contractors and consultants performing work for Sydney Metro.

Department of Transport	NO
Transport for NSW	NO
NSW Trains	NO
Sydney Trains	NO
Sydney Metro	YES
State Transit	NO
Sydney Ferries	NO

3 What is an eligible data breach?

An 'eligible data breach' means:

a) unauthorised access to, or unauthorised disclosure of, personal information held by Sydney Metro where a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or

b) personal information held by Sydney Metro is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur and have the effect described in (a) above.

4 Principles and requirements

3.1 Principles

Sydney Metro proactively encourages and supports staff to respect the privacy of our people and customers by managing their personal information carefully in accordance with our Privacy Management Plan.

Despite this, should an actual or suspected data breach occur, we respond and report promptly and effectively to:

a) maintain public trust and confidence in our ability to handle data and manage personal information in accordance with community expectations
b) respond to a breach promptly to limit the impact of the breach on the agency and on the affected individuals
c) reduce the costs of dealing with a breach
d) ensure compliance with the mandatory notification requirements in Part 6A of the PPIP Act.

3.2 Requirements and preparedness

To support compliance with the PPIP Act and the above principles, Sydney Metro staff must respond to a data breach in accordance with the Sydney Metro Privacy Data Breach Response Procedure which is updated from time to time, and includes the following stages of responding to a data breach:

1. Initial assessment and triage of breach reports.
2. Containing a breach or suspected breach to minimise the possible damage.
3. Assessing or evaluating the information involved in the breach and the risks associated with the breach to determine next steps and implement any additional actions identified to mitigate risks.
4. Notifying individuals / organisations affected by the breach, and the Privacy Commissioner.
5. Post incident review and preventative efforts, based on the type and seriousness of the breach.

The actual breach response is managed by the Privacy Team within Legal Corporate, the Enterprise Security and IT teams (if relevant) and the branch in which the breach occurred. Other areas of Sydney Metro or Transport may be involved if required.

In the event of a data breach involving tax file numbers, the requirements of the Commonwealth Notifiable Data Breaches scheme also apply.

Records of the data breach response should be kept in accordance with the *State Records Act 1998* (NSW). Amongst other things, these records will be used for conducting a post incident review and evaluation.

Sydney Metro and Transport also have controls in place to ensure each is prepared in the event of a data breach:

- Staff training and resources on their obligations under the PPIP and HRIP Acts
- Factsheets and guidance to help staff identify and report a suspected data breach
- Periodic desktop exercises to proactively manage incidents including breaches
- Provisions in template contracts to require suppliers to comply with privacy obligations and notify of suspected breaches
- Audits of some of Transport's more sensitive data holdings;
- Monitoring services (such as dark web monitoring)

5 Compliance and breach of policy

You are required to comply with this policy and its related procedures and standards. If you do not do so, this may result in disciplinary action up to and including termination of your employment or contract.

Appendix A:

1 Sydney Metro accountabilities and responsibilities

Who	
All staff	Comply with the PPIP Act and HRIP Act, including the information protection principles, when handling personal and health information to avoid data breaches. Report any suspected or actual data breach immediately to manager and privacy@transport.nsw.gov.au.
Breach Response Team	Provide advice and management of response to an eligible data breach.
Executive Director of where breach originated	Receive report of possible eligible data breach Decide if data breach is an eligible data breach
Executive Director Legal – Corporate	Accountable for establishing standards, policy, guidelines, advice, training and toolkits to enable Branches to comply with this policy.

2 Related/supporting material

1. Sydney Metro Privacy Data Breach Response Procedure
2. Sydney Metro Privacy Management Plan
3. Privacy and Personal Information Protection Act 1998
4. Health Records and Information Privacy Act 2002

3 Document control

3.1 Superseded documents

Nil. This is a new policy.

3.2 Document history

Date & Policy No	Document owner	Approved by	Amendment notes
4 December 2023	Executive Director Legal – Corporate	Chief Executive	New Policy

3.3 Feedback and help

For advice on interpreting or applying this document, please contact **sydneymetro.privacy@transport.nsw.gov.au**.