Infrastructure NSW

Data Breach Policy

Authorised	Jaime Carragher, Executive Director, Corporate Services
Signature	
Date	June 2026

Table of Contents

1 Definitions

Term	Meaning
Cyber incident	A cyber incident is an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
IT & Cyber Incident Response Plan	a detailed plan outlining the steps to be taken by INSW to contain, assess, investigate and respond to any cyber incident.
Data breach	unauthorised access to, unauthorised disclosure of, personal information held by INSW, or loss of personal information held by INSW in circumstances that are likely to result in unauthorised access to or unauthorised disclosure of the information.
Data Breach Playbook	a detailed plan outlining the steps to be taken by INSW to contain, assess, investigate and respond to a data breach.
Data Breach Response Team	a team comprising senior INSW staff responsible for coordinating INSW's response to a data breach.
Data Breach Triage Team	a team comprising the Privacy Officer (or their nominee) and at least one staff member from the Cyber Security and Compliance team.
Eligible data breach	where there is a data breach and a reasonable person would conclude that the breach is likely to result in serious harm to an individual to whom the personal information relates.
Health information	has the same meaning given to that term in section 6 of the *Health Records and Information Privacy Act 2002* (NSW).
MNDB Scheme	Mandatory Notification of Data Beach Scheme established in section 6A of the *Privacy and Personal Information Protection Act 1998* (NSW).
Personal information	has the same meaning given to that term in section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW). For the purposes of the MNDB Scheme and this Policy, personal information includes health information.
Personal information held by INSW	information that is in the possession or control of INSW, including any user.
Serious harm	occurs where the harm arising from the data breach has, or may, result in a real and substantial detrimental effect on an individual. Harm to an individual includes physical, economic, financial, social, emotional, psychological, or reputational harm.
User	any INSW employee, contractor, volunteer, contracted service provider, consultant, vendor engaged by INSW and any other authorised individual accessing INSW systems, networks and/or information.

2 Policy Statement

2.1 Purpose of the Policy

The purpose of this Data Breach Policy (**Policy**) is to provide a framework for Infrastructure NSW (**INSW**) to comply with its obligations in relation to containing, assessing, managing, notifying and reporting on eligible data breaches under the MNDB Scheme established in Part 6A of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**).

The MNDB Scheme applies to all NSW government agencies and requires agencies to notify the Information and Privacy Commission NSW (**NSW Privacy Commissioner**) and affected individuals if an eligible data breach occurs. The MNDB Scheme only applies to data breaches that are likely to result in serious harm to an individual. If the MNDB Scheme does not apply, notification to individuals or the Privacy Commissioner is not required; however, INSW is still responsible for ensuring any necessary and appropriate response to assess, manage and mitigate the impacts of the data breach.

This Policy has been prepared and is published on the INSW website in accordance with section 59ZD of the PPIP Act and as a requirement under the MNDB Scheme. This Policy was developed with reference to the *Guide to Preparing a Data Breach Policy* issued by the Privacy Commissioner and INSW's Privacy Management Plan.

Why is this Policy important?

Data breaches can have significant consequences for affected individuals; they can give rise to a range of actual or potential harm including financial fraud, identity theft, damage to reputation and even violence.

Responding quickly when a breach occurs can substantially reduce its impact on affected individuals, reduce the costs to agencies of dealing with a breach, and reduce the potential reputational and financial damage that can result.

For these reasons, it is important that INSW documents and implements a policy to ensure it can quickly and effectively respond to and manage data breaches.

3 Who does this Policy apply to?

All INSW users must comply with this Policy, including:

- all INSW permanent, temporary or seconded employees, contractors, consultants or agency staff who work on a full time, part time, or volunteer basis;
- any person authorised to access INSW information systems and assets;
- any consultants and persons or organisations authorised to administer, develop, manage and support INSW information systems and assets; and
- third party suppliers, vendors, and hosted/managed service providers.

Failure to comply may result in corrective action, including misconduct action.

4 Response and Management Strategy

4.1 What is a data breach?

A data breach occurs when personal information, including health information, held by INSW is lost or subject to unauthorised access or unauthorised disclosure.

A data breach can be accidental or intentional and may arise because of a cyber-attack, inadvertent disclosure, broad access to sensitive systems, or loss or theft of a physical device.

Data breaches include (but are not limited to):

- loss or theft of a device containing INSW information, for example a loss of a laptop;
- an INSW database or information repository being compromised or accessed without authorisation, for example the sharing of user login details with a third party, hacking or malware infection;
- unauthorised transfer of INSW information to external storage devices, systems and applications; or
- an INSW staff member mistakenly providing personal information to an unauthorised person or entity, for example by sending an email containing personal information to the wrong recipient.

4.2 How INSW has prepared for Data Breaches

Training and awareness

INSW takes privacy seriously and requires all users to complete an annual mandatory e-learning module “INSW Privacy and Personal Information”, which contains sections on the MNDB Scheme. This module ensures that staff are aware of privacy principles and requirements that apply to INSW under the PPIP Act.

Identifying and reporting data breaches

Identification and response

The quicker an agency can detect a data breach, the better the chance that it may be contained and potential harms mitigated through prompt action.

INSW staff and members of the community can report actual or suspected data breaches by emailing the Privacy Officer at privacy@infrastructure.nsw.gov.au as soon as reasonably practicable, preferably within 24 hours. All relevant information must be provided about the type of data breach, when it occurred and how it transpired. If the data breach also involves a potential cyber incident, all staff members must report the breach as soon as possible to the appropriate member in the Cyber Security and Compliance team.

Data Breach Playbook

INSW has created a robust Data Breach Playbook which sets out the specific steps INSW will take to respond efficiently and expediently to data breaches.

INSW staff should consult the Data Breach Playbook for detailed guidance on how to report, escalate and respond to an actual or suspected data breach.

The Data Breach Playbook should be used in conjunction with the IT & Cyber Incident Response Plan.

Managing third party risks

All INSW contractors who hold, manage or use personal information for or on behalf of INSW are subject to privacy obligations, including requirements to:

- handle data breaches in accordance with the PPIP Act; and
- immediately notify INSW of any data breach or any actual or suspected data breach involving the inadvertent or malicious loss, disclosure or corruption of INSW information.

Regular testing and review

INSW will regularly review, test and update this Policy and the Data Breach Playbook to ensure it remains fit for purpose.

The Information and Privacy Commission NSW advises that regular testing of an agency's data breach response process is the best way to ensure that all relevant staff understand their roles and responsibilities, and to check that details of the response process are current. Testing may involve the development of a hypothetical or test incident and a review of how the agency manages the event.

4.3 Containing, assessing, and managing eligible data breaches

Reasonable steps to prevent or mitigate losses

In the event of a data breach, users are required to follow all directions to prevent any further loss or compromise of personal information and minimise any potential harm to affected individuals.

Assessment of the Data Breach

The Data Breach Triage Team will conduct an initial assessment of the data breach and consider whether the breach is an eligible data breach (as defined in section 1 of this Policy). The Data Breach Triage Team will consider any relevant guidelines issued by the NSW Privacy Commissioner under section 59ZI of the PPIP Act in conducting its assessment.

The Data Breach Response Team

If the Data Breach Triage Team suspects the breach is an eligible data breach, they will establish a Data Breach Response Team. The members of the Response Team are listed on the "Privacy at INSW" intranet page.

The Response Team will:

- take steps to identify the underlying cause of the data breach;
- assess the risk of serious harm to affected individuals; and
- recommend steps to mitigate the risk of serious harm from, arising or continuing from the data breach (considering the type and sensitivity of the compromised data).

The Response Team will consider any relevant guidelines issued by the Privacy Commissioner under section 59ZI of the PPIP Act in conducting its assessment.

The Privacy Officer will prepare an assessment report and advise the Chief Executive (or their delegate) regarding notifications to the NSW Privacy Commissioner and affected individuals.

Mandatory notification of Eligible Data Breaches

If a data breach is assessed as 'eligible', the Privacy Officer must notify:

- the NSW Privacy Commissioner immediately; and

- affected individuals as soon as practicable, unless a relevant exemption applies, using the template in the Data Breach Playbook or IT & Cyber Incident Response Plan.

Depending on the circumstances of the data breach and the categories of data involved, agencies may need to notify or engage with other State or Federal agencies or third parties.

Post Data Breach Review

The purpose of a Post Incident Report is to identify lessons learned and make recommendations about remediating any processes or weaknesses in data handling that may have contributed to the breach and whether any changes are required following a data breach to mitigate or prevent future risks.

Once the data breach response is finalised and notifications complete, the Privacy Officer will conduct a Post Incident Review with the relevant Business Unit and complete a Post Incident Report for the Chief Executive.

Registers

The Privacy Officer will maintain a public notification register of all eligible data breaches impacting INSW on the INSW website. This will be used to provide public notifications of eligible data breaches where INSW is unable to notify, or it is not reasonably practicable to notify, affected individuals.

INSW will also keep an internal register of all data breaches (not just those that meet the test of an eligible data breach under the PPIP Act). This is to ensure a central record of key risk areas and vulnerabilities, to ensure continuous review and improvement of INSW's information management systems. The Privacy Officer will be responsible for managing and updating the internal register.

Proactive identification

INSW proactively identifies data breaches that may impact INSW information by auditing and monitoring public domains and compliance with contractual obligations by third party suppliers, vendors and hosted/managed service providers.

5 Relevant Legislation and Documents

This Policy complies with the requirements of the:

- *Privacy and Personal information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- Guidelines issued by the NSW Privacy Commissioner (listed below)

This Policy is to be read in conjunction with:

- INSW IT & Cyber Incident Response Plan
- INSW Data Breach Playbook
- INSW Privacy Management Plan

This Policy aligns with relevant obligations and procedures set out in:

- INSW Acceptable Use Policy
- INSW Access Control Policy
- INSW Information Security Policy

- INSW Records & Information Management Policy
- INSW Risk Management Guidelines

Guidelines issued by the NSW Privacy Commissioner:

- *Guide to preparing a data breach policy* (May 2023)
- *Guide to managing data breaches in accordance with the PPIP Act* (updated July 2024)
- *Guide to Regulatory Action under the MNDB scheme* (August 2023)
- *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* (September 2023)
- *Guidelines on the exemption for risk of serious harm to health or safety under section 59W* (September 2023)
- *Guidelines on the exemption for compromised cyber security under section 59X* (September 2023)

6 Document Status

Title	Data Breach Policy
Version	4.0
Effective date	June 2026
Author	Privacy Officer Associate Director, Cyber Security and Compliance
Authorised by	Executive Director, Corporate Services
Next review date	June 2028

7 Revision History Log

Version #	Revision Date	Author	Changes
1.0	28/11/2023	Director, Legal / Privacy Officer	Initial publication to ensure INSW compliance with introduction of the MNDB Scheme
2.0	05/12/2024	Director, Legal / Privacy Officer Associate Director, Cyber Security and Compliance	Updated intranet page name to “Privacy at INSW” Updated documents information
3.0	04/12/2025	Director, Legal Associate Director, Cyber Security and Compliance	Updated plan name to “IT & Cyber Incident Response Plan”
4.0	25/06/2026	Privacy Officer Associate Director, Cyber Security and Compliance	Updates to definitions, timeframe for notification of data breaches, role and responsibilities of Privacy Officer and contact details