
Data Breach Policy


Authorised	Tom Gellibrand, Chief Executive
Signature	
Date	27 November 2023

Table of Contents

1	Definitions	3
2	Policy Statement	4
2.1	Purpose of the Data Breach Policy.....	4
2.2	Why is a Data Breach Policy necessary?	4

3	Who does this Policy apply to?	4
4	Response and Management Strategy	5
4.1	What is a Data Breach?	5
4.2	How INSW has prepared for Data Breaches.....	5
4.3	Containing, assessing, and managing Eligible Data Breaches.....	6

5	Relevant Legislation and Documents	8
----------	---	----------

1 Definitions

Term	Meaning
Cyber incident	an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by 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, or loss of, Personal Information held by INSW
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 and at least one executive from a team affected by the Data Breach.
Eligible Data Breach	where there is a Data Breach and a reasonable person would conclude that the Data Breach is likely to result in serious harm to an individual to whom the Personal Information relates.
Health Information	a class of personal information and includes information or opinions about the health or disability of an individual and/or a patient's wishes about future healthcare. It also includes information collected in connection with the provision of a health service.
MNDB Scheme	Mandatory Notification of Data Beach Scheme, established in section 6A of the <i>Privacy and Personal Information Protection Act 1998</i> (NSW) (commenced 28 November 2023).
Personal Information	has the same meaning given to that term in the PPIP Act, being 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, and for the purposes of the MNDB Scheme includes Health Information.
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 Data Breach Policy

The purpose of this policy is to provide a framework for Infrastructure NSW's (INSW) to comply with its obligations under the Mandatory Notification of Data Breach Scheme (MNDB Scheme) established in Part 6A of the Privacy and Personal Information Protection Act 1998 (PPIP Act).

The MNDB Scheme commenced on 28 November 2023, requiring all public sector agencies, including INSW, to take various steps to contain, assess, manage, notify, and report on eligible data breaches.

This policy was developed with reference to the *Guide to Preparing a Data Breach Policy* issued by the Privacy Commissioner in May 2023.

This policy complies with section 59ZD of the PPIP Act and is published on the INSW website.

2.2 Why is a Data Breach Policy necessary?

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 plan 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.

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.

Types of data breaches include:

- 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,
- 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 suspected Data Breaches

Importance of quick 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 can report suspected or actual Data Breaches by Completing the data breach form on the Privacy intranet page. Alternatively, INSW staff may directly contact the staff listed on the INSW Privacy intranet page as privacy contacts.

If members of the community wish to report a suspected or actual Data Breach impacting INSW data or systems, they can email Privacy@infrastructure.nsw.gov.au. Please provide your contact details so the Privacy Officer can contact you if further information is required.

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 INSW Data Breach Playbook for detailed guidance on how to report, escalate and respond to a suspected Data Breach. The Data Breach Playbook is available on the intranet.

The Data Breach Playbook should be used in conjunction with the 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,
- immediately notify INSW of any Data Breach or any suspected or alleged Data Breach involving the inadvertent or malicious loss, disclosure or corruption of INSW information.

Annual testing and review

INSW understands that a data breach policy will only be effective if it is current, well communicated and implemented. INSW will annually review, test, and update this Policy and the Data Breach Response Playbook to ensure it remains fit for purpose.

The IPC 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

Notification of *all* suspected or actual Data Breaches

All Data Breaches are to be notified to the Privacy Officer. Data Breaches should be reported **as soon as possible, but within two working days**.

INSW staff should report an actual or suspected Data Breach by using the form on the Privacy intranet page.

If **members of the community** wish to report a suspected or actual Data Breach impacting INSW data or systems, they can email Privacy@infrastructure.nsw.gov.au. Please include your contact details so the Privacy Officer can contact you if further information is required.

Reasonable steps to prevent or mitigate losses

In the event of a Data Breach, Users are immediately required to take all reasonable steps to prevent any further loss or compromise of personal and/or health information and minimise any potential harm to affected individuals.

Assessment of the Data Breach

The Data Breach Triage Team will conduct a thorough assessment of the suspected Data Breach and consider whether the suspected Data Breach is an *Eligible* Data Breach. The Data Breach Triage Team will consider any relevant guidelines issued by the Privacy Commissioner under section 59ZI of the PPIP Act in conducting its assessment.

What is an *Eligible* Data Breach?

A data breach will be considered an Eligible Data Breach if the breach is **likely to result in serious harm** to affected individuals.

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.

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 '**Response Team**'). The members of the Response Team are listed on the INSW Privacy 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,
- recommend steps to mitigate the risk of serious harm from arising or continuing (considering the type and sensitivity of the compromised data),
- provide advice to the Chief Executive of INSW or their delegate regarding notifications to affected individuals and / or the Privacy Commissioner of NSW.

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

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 Cyber Incident Response Plan and/or Data Breach Playbook.

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.¹

Post Data Breach Review

Once the incident response is finalised and notifications complete, the relevant Business Unit will be responsible for conducting a Post Incident Review and completing a Post Incident Report which must be sent to the Response Team for input before finalisation and reporting to the Chief Executive Officer and the INSW Audit and Risk Committee. The purpose of the Post Incident Report is to identify and make recommendations about remediating any processes or weaknesses in data handling that may have contributed to the breach.

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 personal information management systems.

¹ Such as: NSW Police Force, Department of Customer Service, Cyber Security NSW, The Office of the Australian Information Commissioner, Australian Federal Police, The Australian Taxation Office, The Australian Digital Health Authority, The Department of Health, The Office of the Government Chief Information Security Officer, The Australian Cyber Security Centre, Any third-party organisations or agencies whose data may be affected, Financial services providers, Professional associations, regulatory bodies or insurers, Foreign regulatory agencies.

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)
- Guidelines issued by the Privacy Commissioner

This Policy is to be read in conjunction with:

- INSW 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 Cybersecurity Policy
- INSW Records & Information Management Policy
- INSW Information Security Management System Policy
- INSW Risk Management Guidelines

- Guides and 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* (June 2023)
- *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)

Document Status

Title	Data Breach Policy
Version	1.0
Effective date	28 November 2023
Author	Director, Legal / Privacy Officer
Authorised by	Executive Director, Corporate Services
Next review date	November 2024

Revision History Log

Version #	Revision Date	Author	Changes
1.0	28 November 2023	Director, Legal / Privacy Officer	First version to ensure INSW compliance with Introduction of the MNDB Scheme