Data Breach Policy

Version number: 1.0

28 November 2023

Acknowledgement of Country

Service NSW acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to Elders past and present and acknowledge the Aboriginal and Torres Strait Islander people that contributed to the development of this Policy.

Data Breach Policy

Published by Service NSW

service.nsw.gov.au

First published: November 2023

Copyright and disclaimer

Information contained in this publication is based on knowledge and understanding at the time of writing, November 2023, and is subject to change. For more information, please visit the Service NSW Copyright and Disclaimer.

Content

1 **Policy Statement** 1

1.1 Objectives 1

1.2 Scope 1

1.2.1 Partner Agency information 1

1.2.2 Third parties and jointly held personal information 2

2 **How we prepare for data breaches** 3

2.1 Policies and procedures 3

2.2 Training and awareness 3

3 **What happens if we have a data breach?** 5

3.1 What is an 'eligible data breach'? 5

3.2 How we respond to data breaches 6

3.2.1 Reporting and containing suspected eligible data breaches 6

3.2.2 Data Breach Management Team 6

3.2.3 Cyber-attacks & system compromise 6

3.2.4 Assessing a suspected eligible data breach 6

3.2.5 Notifying an eligible data breach 6

3.2.6 Non-eligible data breaches 7

3.2.7 Maintaining registers 7

3.2.8 Post-breach evaluation, review and reporting 7

3.2.9 Records management 7

4 **Roles & responsibilities** 8

4.1 Roles and responsibilities of staff 8

4.1.1 All staff 8

4.1.2 People Leaders (team leaders and managers) 8

4.1.3 Privacy Team 8

4.1.4 Partnership Managers 8

4.1.5 Data Breach Management Team 8

4.1.6 Cyber Security Team 8

4.1.7 Information Governance 9

4.1.8 DCS Brand, Digital and Communications team 9

4.1.9 DCS People and Culture 9

4.1.10 DCS Governance, Risk and Assurance 9

4.1.11 DCS Legal 9

4.2 Engaging with external stakeholders & entities 9

4.3 Contacting Service NSW 10

5 Related Policies and Documents ... 11

6 Glossary of terms ... 12

7 Document Control ... 15

7.1 Document Approval ... 15

7.2 Document Version Control ... 15

7.3 Review Date ... 15

1 Policy Statement

This Data Breach Policy (Policy) sets out how Service NSW responds to and manages eligible data breaches in line with the Mandatory Notification of Data Breaches Scheme (MNDB Scheme) established under the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).

1.1 Objectives

As a 'single front door' for customers accessing government services, Service NSW is a trusted guardian of personal information for our customers.

Service NSW is committed to ensuring the confidentiality, integrity and availability of customer data. We protect personal information by taking proactive measures to prevent data breaches. We will respond quickly and effectively when a breach occurs and take action to minimise harm to our customers and our people.

Service NSW staff (staff) must follow the internal **Service NSW Data Breach Response Plan** (Response Plan) for detailed guidance on how to respond to data breaches.

Service NSW is an executive agency related to the Department of Customer Service. Service NSW is a separate public sector agency from DCS for the purpose of privacy legislation, but does rely on DCS for some corporate and governance services.

Please refer to the Glossary of terms below for definitions of key terms which appear in bold throughout this Policy.

1.2 Scope

This Policy applies to all staff, including third parties engaged to handle personal information on our behalf.

References to personal information include health information under the *Health Records and Information Privacy Act 2002* (NSW).

This Policy applies only to data breaches that involve personal information held by Service NSW, which includes personal

- in the possession or control of Service NSW or a person employed or engaged by the agency in the course of their employment or engagement, or
- which is contained in a State Record in respect of which the agency is responsible under the *State Records Act 1998* (NSW) (State Records Act).

Personal information can be 'jointly held' by more than one agency or entity.

1.2.1 Partner Agency information

Most personal information Service NSW handles is for the purpose of fulfilling a customer transaction on behalf of a **Partner Agency**.

Depending on the circumstances, Service NSW and a Partner Agency may both have privacy obligations in respect of the same information under the MNDB Scheme, and a role to play in responding to and managing a data breach, including identifying all affected individuals.

Where a breach involving personal information collected for or on behalf of a Partner Agency (Partner Agency information) occurs, we will determine how to comply with our privacy obligations in collaboration with the relevant Partner Agency. Generally, only one agency is required to notify affected individuals of an eligible data breach involving multiple agencies, provided

- the data breach involves more than one agency,
- each agency has undertaken an assessment of the breach,
- the head of each agency has made a data breach notification to the Privacy Commissioner, and
- the other agency involved in the breach has undertaken to notify affected individuals of the eligible data breach.

1.2.2 Third parties and jointly held personal information

All third-party contractors are subject to privacy obligations and must handle personal information in line with the PPIP Act. Service NSW must be advised as soon as a contractor becomes aware of a data breach involving personal information being handled on behalf of Service NSW.

2 How we prepare for data breaches

Service NSW takes proactive measures to prevent, detect and respond to data breaches.

We take all reasonable security measures to protect personal information from unauthorised access, unauthorised disclosure and loss. For example, we

- work with Cyber Security NSW to ensure an integrated approach in preventing cyber security threats and safeguarding personal information
- align our framework for protecting data with the Cyber NSW Cyber Security Policy and the Australian Cyber Security Centre's Essential Eight strategies to mitigate cyber security incidents
- are continuously improving cyber risk management processes and operations to effectively manage cyber risks,
- create a privacy and cyber aware culture amongst staff through regular cyber security awareness campaigns, including phishing simulations, privacy and cyber training and targeted communications to uplift staff maturity
- use multi-factor authentication for access by Service NSW staff to our systems, and physical measures, such as floor, building and equipment security to safeguard personal information
- conduct cyber security incident simulations, allowing Service NSW to be better prepared to respond to suspected or actual data breaches in a coordinated and effective manner.

Service NSW also implements various tools to assist customers, including a breached password service to check customers passwords against a database of known compromised passwords published online.

We ensure that personal information is not kept longer than necessary and is disposed of appropriately and in line with our obligations under the State Records Act.

2.1 Policies and procedures

All staff are required to and encouraged to report data breaches, and a positive reporting culture is supported across Service NSW.

We have a comprehensive Response Plan and range of policies and procedures in place to assist staff to respond to data breaches. Related policies and documents are listed below and these policies are aligned with this Policy where appropriate.

We will review the Policy and the Response Plan yearly and test the plan every 2 years.

We use Privacy Threshold Assessments and Privacy Impact Assessments to operationalise privacy by design principles for projects, systems and service delivery changes that involve new or changed ways of handling personal information, and undertake a range of assurance activities to embed privacy across Service NSW.

2.2 Training and awareness

We prepare for data breaches by delivering mandatory privacy training for our people, so they understand their privacy obligations and how to protect personal information. This includes a section on cyber security awareness, the MNDB Scheme and how to respond to suspected eligible data breaches.

We have guidance and factsheets available for staff to help them identify and report suspected data breaches.

We take a range of proactive measures to raise staff awareness including phishing simulations and business continuity exercises We also provide additional privacy training and awareness for those staff who work in areas with a higher exposure to the personal information of customers or staff.

3 What happens if we have a data breach?

3.1 What is an ‘eligible data breach’?

A **data breach** occurs when:

- there is unauthorised access to, or unauthorised disclosure of personal information held by Service NSW, OR
- personal information held by Service NSW is lost in circumstances where the loss is likely to result in unauthorised access to, or disclosure of, the information.

An **eligible data breach** occurs when:

- there is a **data breach**, AND
- a reasonable person would conclude that the unauthorised access to, or unauthorised disclosure of, the personal information would be likely to result in serious harm to an individual to whom the information relates.

Serious harm occurs where the harm arising from the eligible 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.[1]

Assessment of the likelihood of serious harm arising from a data breach is an objective test. The phrase ‘likely to result’ means that the risk of serious harm to an individual is more probable than not, rather than merely possible.[2]

Data breaches may

- occur between agencies, within Service NSW or externally, for example with a contractor
- arise due to a technical problem, system change or upgrade, human error, inadequate policies and training, a misunderstanding of the law or a deliberate act
- involve information that is held in both digital and hard copy records.

Examples of data breaches include

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by someone who is not authorised to access the information, including staff
- inadvertent disclosure of personal information due to ‘human error’, for example an email sent to the wrong person or publishing personal information on the internet.

[1] IPC Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act [para 3.2].

[2] IPC Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act [para 3.3].

3.2 How we respond to data breaches

We have a comprehensive Response Plan that contains detailed steps and procedures that staff must take in the event of a data breach. All staff are expected to be familiar with the Response Plan and understand how to escalate and respond to a data breach.

3.2.1 Reporting and containing suspected eligible data breaches

All staff and people leaders are responsible for taking immediate, common-sense steps to contain the breach, and must immediately report suspected eligible data breaches to their manager or team leader, and report these to the Privacy Team following internal processes for reporting a data breach.

Service NSW will take all reasonable steps to contain data breaches, minimise the risk of harm to individuals and prevent further data breaches occurring.

3.2.2 Data Breach Management Team

Depending on the nature of the breach, a **Data Breach Management Team** (DBMT) may be formed to conduct a detailed investigation. The DBMT includes representatives appropriate to respond to the breach, including individuals who may be required to further investigate and respond to the breach. The DBMT assists to determine and action any containment steps.

3.2.3 Cyber-attacks and system compromise

The Cyber Security Team at Service NSW actively monitors and detects data breaches. Where it appears a data breach has occurred because of a suspected cyber-attack or system compromise, staff should immediately contact the NSW Cyber Security Team for advice and assistance in containing and preventing reoccurrence of the breach. Service NSW will advise and consult with Cyber Security NSW when necessary.

3.2.4 Assessing a suspected eligible data breach

Once a suspected eligible data breach is reported it is considered by an Assessor. We will immediately make all reasonable efforts to contain the breach and mitigate harm arising from the data breach.

We will expeditiously (and **within 30 calendar days**) carry out an assessment of whether the data breach is, or there are reasonable grounds to believe that the data breach is an eligible data breach. We do this in line with the requirements of the MNDB Scheme, and relevant guidance issued by the Information and Privacy Commission NSW (IPC).

The Assessor must consider the *IPC Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* (as updated from time to time) when assessing a suspected eligible data breach.

If an assessment cannot reasonably be conducted within 30 calendar days (for example if there is a complex cyber-attack and an investigation is still under way), the period to conduct the assessment may be extended. We must notify the Privacy Commissioner of any extension.

All data breaches are different and will be assessed on a case-by-case basis.

3.2.5 Notifying an eligible data breach

If a breach is assessed and found to be an eligible data breach, we will immediately notify the Privacy Commissioner and affected individuals as soon as practicable (unless an exemption applies).

The Response Plan contains detailed guidance about how to notify affected individuals. At all times Service NSW's key priority is to support our customers and our people and mitigate any harm that may arise.

There are some limited exemptions under the MNDB Scheme where Service NSW may not be required to notify. Service NSW will be exempt from notifying where another agency has undertaken to notify for the same breach.

If an exemption is relied upon, we will notify the Privacy Commissioner.

3.2.6 Non-eligible data breaches

There may be circumstances where it may be necessary for Service NSW to notify under another legislative Scheme, or on a voluntary basis.

We will notify breaches:

- involving Tax File Numbers that are assessed as meeting the threshold of an 'eligible data breach' under the *Privacy Act 1988* (Cth) to the **Office of the Australian Information Commissioner** (OAIC)
- involving personal information received under the *Data Sharing (Government Sector) Act 2015* (NSW) to the IPC.

We may also notify individuals on a voluntary basis – i.e., where the breach is not likely to result in serious harm to an individual. This will depend on the circumstances of the breach, and may happen

- to be transparent to our customers when something has gone wrong, for example where we need to contact a customer about a transaction such as reissuing a licence or permit
- to prevent an immediate and foreseeable harm to the individual
- where a customer has raised the handling of their personal information by Service NSW.

Sometimes, notifying individuals of minor breaches can cause undue stress or harm. We will also consider any unintended consequences when deciding whether to notify individuals on a voluntary basis.

3.2.7 Maintaining registers

All eligible data breaches will be listed in Service NSW's Internal Register of eligible data breaches.

Where it is not possible or reasonably practicable to notify affected individuals directly about the eligible data breach, we will notify by placing a public notice on our website and taking reasonable steps to publicise this notification.

Details of public notices will be maintained in Service NSW's Data Breach Notification Register for at least 12 months after the date the notification is published.

3.2.8 Post-breach evaluation, review and reporting

We will undertake a post-breach review and evaluation for all eligible data breaches to determine why the breach occurred and how Service NSW responded. We will document this review to identify appropriate controls to reduce the risk of similar breaches occurring in the future.

3.2.9 Records management

Service NSW maintains records for all suspected eligible data breaches, and keeps information in line with our obligations under the State Records Act. We review and report on data breaches, and track and implement controls within the Service NSW enterprise risk register.

This Policy will be reviewed at annually and updated as required.

4 Roles & responsibilities

4.1 Roles and responsibilities of staff

4.1.1 All staff

All staff must be aware of their obligations under the MNDB Scheme. Staff must advise their people leader immediately when they suspect an eligible data breach has occurred, and act on any advice from their people leader and the Privacy Team or the DBMT to contain the breach.

4.1.2 People Leaders (team leaders and managers)

Service NSW people leaders are responsible for identifying what information was disclosed and the cause of the breach, assisting staff to take immediate common sense steps to contain the breach, and escalating the breach to the Privacy Team.

People leaders may be required provide additional information, take further actions to contain and mitigate the breach, participate in any DBMT and implement controls to reduce the risk of reoccurrence.

4.1.3 Privacy Team

Service NSW has a dedicated Privacy Team that is responsible for privacy management across Service NSW. This includes managing this Policy, our Response Plan and guidance material, and providing specialist advice and assistance when a suspected eligible data breach occurs.

The Privacy Team participates in and may convene a DBMT, and is responsible for ensuring decisions are made consistently with the MNDB Scheme by taking action or seeking necessary approvals in line with Service NSW Delegations made under the PPIP Act.

4.1.4 Partnership Managers

If the breach involves a Partner Agency, the Partnership Manager plays a key role in co-ordinating Service NSW's response, participates in the DBMT, and acts as a conduit between Service NSW and the Partner Agency.

4.1.5 Data Breach Management Team

The purpose of a DBMT is to respond to complex or higher risk breaches.

The DBMT is made up of those people within Service NSW who are best placed to investigate and respond. It may also include representatives from the Department of Customer Service or a Partner Agency, as required.

4.1.6 Cyber Security Team

Responsible for coordinating responses to cyber security incidents that have a high impact on Service NSW. The Cyber Security team may provide advice on the root cause of the breach, the steps required to contain and remediate the breach, and recommend steps as part of post-incident review. They may also participate in or convene the DBMT as required, and assist to engage external specialist expertise where required.

4.1.7 Information Governance

Information Governance will assist to respond to breaches that raise issues of data governance and take necessary actions and engage with stakeholders to improve organisational practices.

4.1.8 DCS Brand, Digital and Communications team

Assists Service NSW to communicate with the public about significant data breaches, including reviewing any public statements and other internal and external communications.

4.1.9 DCS People and Culture

Provides support to staff and people leaders when a breach occurs where required and oversees the adherence to the DCS Code of Ethics and Conduct by staff.

4.1.10 DCS Governance, Risk and Assurance

Where a data breach may have a high impact on Service NSW and DCS Governance, Risk and Assurance will have a role in coordinating data breach response in line with the requirements of the MNDB Scheme.

4.1.11 DCS Legal

Responsible for assisting Service NSW with complex breaches where there is a need for legal advice.

4.2 Engaging with external stakeholders & entities

It may be necessary for Service NSW to engage with other agencies or organisations when a data breach occurs. This may include but is not limited to

- ID Support for contact detail verification or enrichment and notification assistance, particularly where there is potential identity compromise
- Cyber Security NSW, the DCS Chief Information Security Officer and the Australian Cyber Security Centre in relation to suspected or actual cyber-attacks
- regulators including the IPC and the OAIC
- the NSW Police Force, Australian Federal Police when there is suspected criminal or fraudulent activity
- other government agencies, third-party organisations or Partner Agencies
- entities that may assist in responding to a breach, including external providers such as legal advisers and other experts such as forensic and privacy specialists.

4.3 Contacting Service NSW

For any questions or feedback about this policy, or to report a suspected data breach impacting Service NSW data or systems, please contact the Privacy Team.

Phone: 13 77 88

Email: privacy@service.nsw.gov.au

Website: www.service.nsw.gov.au/privacy

Mail: Service NSW Privacy Officer
Risk, Strategy and Customer Support
GPO Box 7057
Sydney NSW 2001

5 Related Policies and Documents

5.1.1 Service NSW

Data Breach Response Plan

Cyber Incident Response Plan

Service NSW Privacy Management Plan

Service NSW's Privacy Management Framework

5.1.2 Department of Customer Service

Information Security Policy

Code of Ethics and Conduct

IT Acceptable Use Policy

5.1.3 Information and Privacy Commission

Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act

Guide to managing data breaches in accordance with the PPIP Act

5.1.4 Digital.NSW

NSW Cyber Security Policy

5.1.5 Reconstruction Authority

NSW State Emergency Management Plan

6 Glossary of terms

Terms used in this document have the same meaning as they carry in the PPIP Act, unless otherwise indicated.

6.1.1 Affected individuals

An individual:

- to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and
- who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.

Has the same meaning given under section 59D(2) of the PPIP Act.

6.1.2 Data breach

A data breach occurs where personal information held by Service NSW 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 of the information.

6.1.3 Data Breach Policy (Policy)

Service NSW's Data Breach Policy required to be published on Service NSW's website.

6.1.4 Data Breach Response Plan (Response Plan)

Service NSW Data Breach Response Plan (internal document guiding staff in the event of a data breach).

6.1.5 Eligible Data Breach (EDB)

An eligible data breach occurs when there is a **data breach** and a reasonable person would conclude that the unauthorised access to, or unauthorised disclosure of, the personal information would be likely to result in serious harm to an individual to whom the information relates.

Has the same meaning given under section 59D of the PPIP Act.

6.1.6 Health information

Has the same meaning given under section 6 of the *Health Records and Information Privacy Act 2002*.

Includes information or an opinion about an individual's physical or mental health or a disability and information connected to the provision of a health service. It includes healthcare identifiers.

Note: For the purposes of the MNDB Scheme, the definition of 'personal information' includes 'health information'.

6.1.7 MNDB Scheme

Mandatory Notification of Data Breaches Scheme established under Part 6A of the PPIP Act.

6.1.8 Partner Agency

A NSW Public Service agency, a NSW local government authority, Commonwealth agency, other State or Territory government agency or non-government entity that Service NSW exercises functions for under delegation or by agreement.

6.1.9 Personal information

Has the same meaning given under sections 4 and 59B of the PPIP Act.

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.

Personal information may include:

- identifying information, such as name, date of birth, residential address, email address, phone number
- credit card numbers, account numbers, licence numbers, vehicle registration number, passport numbers, tax file numbers
- sex, gender, ethnicity and cultural background
- photographs, video images, audio recordings (including call recordings)
- call notes, case notes, and information held in systems or databases about an individual who is able to be identified
- biometric information such as fingerprints and facial biometrics
- health information such as information about an individual's physical or mental health, disability and information connected to the provision of a health service.

6.1.10 PPIP Act

Privacy and Personal Information Protection Act 1998 (NSW)

6.1.11 Serious harm

Refer to IPC *Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act* (as updated from time to time) on what is 'serious harm' as the term is not defined in the PPIP Act.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

6.1.12 Service NSW staff (staff)

Service NSW staff includes:

- all Service NSW permanent full time, part time, trainee and temporary employees and approved users of Service NSW information systems and assets, including contingent labour from labour hire, contractors and consultants, performing work for Service NSW.
- any person, organisation or agency authorised to administer, develop, manage and support Service NSW Information systems and assets

- third party suppliers, vendors and hosted/managed service providers that handle personal information.

7 Document Control

7.1 Document Approval

Name and Position	Date
Catherine Ellis SNSW Chief Risk Officer Executive Director Risk, Strategy & Customer Support	21 November 2023

7.2 Document Version Control

Version	Status	Date	Prepared By	Comments
1.0	Draft	15 November 2023	Privacy Team	Final

7.3 Review Date

This policy will be reviewed in **November 2024**.

It may be reviewed earlier in response to post-implementation feedback from Business Units.

2-24 Rawson Place
Sydney NSW 2000

Office hours:
Monday to Friday
9.00am to 5.00pm

T: 13 77 88
E: privacy@service.nsw.gov.au
W: www.service.nsw.gov.au