New South Wales Crime Commission

# NSW Crime Commission

# Data Breach Policy

*November 2023*

New South Wales Crime Commission

## Document Control

This document is only valid on the day it was printed.
The source of the document is located with the ISMS documentation in Objective

| Authors | Policy No. |
|---|---|
| NSW Crime Commission | **ICT2023/10** |

**Version History**

| Date | Version | Revision History | Author /Reviser |
|---|---|---|---|
| October 2023 | V0.1 | First draft | NSW Crime Commission |
| | | | |

**Document Reviews**

| Date | Version | Comments | Reviewed by |
|---|---|---|---|
| | V0.1 | | |
| | | | |

**Approvals**

This document requires the following approvals.

| Name | Title | Date of Issue | Version |
|---|---|---|---|
| | Chief Operating Officer | 22/11/23 | V1.0 |
| | | | |

| | |
|---|---|
| **Responsible Business Group:** | Corporate and Enterprise Services |
| **Distribution:** | |
| **Content Security:** | OFFICIAL |

# Contents

# 1 Introduction

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 every NSW public sector agency bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of eligible data breaches. Under the scheme, public sector agencies are required to prepare and publish a Data Breach Policy (DBP) for managing such breaches as well as maintaining an internal register and public register of eligible data breaches.

This policy outlines the New South Wales Crime Commission's (the Commission) approach to complying with the MNDB Scheme, the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

# 2 Scope

This policy applies to all staff and contractors of the Commission. This includes temporary and casual staff, private contractors and consultants engaged by the Commission to perform the role of a public official. This policy also applies to third party providers, who hold personal and health information on behalf of the Commission.

This policy will be reviewed in 12 months' time or where improvements are identified in response to a data breach whichever occurs sooner.

# 3 Purpose

The purpose of this policy is to provide guidance to Commission staff on data breaches of Commission held data in accordance with the requirements of the PPIP Act.

This policy sets out how the Commission will respond to data breaches involving personal information. The Commission acknowledges that not all data breaches will be eligible data breaches but regardless the Commission takes all data breaches seriously. The policy details:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches

Effective breach management, including notifications, assists the Commission in avoiding or reducing possible harm to both the affected individuals / organisations and the Commission, and may prevent future breaches.

## 4 Roles and Responsibilities

The following staff have identified roles under the DBP:

- The **Chief Operating Officer** is responsible for implementing this Policy, reporting data breaches to the Commissioner, all notifications and actions for eligible data breaches and advice on the communication strategy and messaging to affected individuals and external reporting agencies.
- The **Privacy Officer** is responsible for investigating data breaches, preparing the Data Breach Report and Action Plan and maintaining the internal and public registers for data breaches.
- The **Chief Information Officer** will provide advice on technical steps required to mitigate a data breach where applicable.
- All **Commission employees** have a responsibility for immediately reporting a suspected data breach in accordance with this policy.

All staff and contractors have a responsibility to notify the Chief Operating Officer of any data breaches within one business day of becoming aware that a data breach has occurred and provide information about the data breach.

## 5 What is an Eligible Data Breach?

The definition of personal information for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act).

This means that for the purposes of the MNDB Scheme, **'personal information'** means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion and includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

A data breach occurs when personal information held by an agency (whether held in digital or hard copy) 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.

This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or unauthorised sharing of personal information between teams within an agency may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error. A data breach may also occur because of a misconception about whether a particular act or practice is permitted under the Information Protection Principles (IPPs).

Examples of data breaches include:

- ***Human error***
    - When a letter or email is sent to the wrong recipient.
    - When system access is incorrectly granted to someone without appropriate authorisation.
    - When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
    - When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information
- ***System failure***
    - Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
    - Where systems are not maintained through the application of known and supported patches.
- ***Malicious or criminal attack***
    - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
    - Social engineering or impersonation leading into inappropriate disclosure of personal information.
    - Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
    - Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

The MNDB Scheme applies where an 'eligible data breach' has occurred. For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are two tests to be satisfied:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, **and**
2. 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.

The term **'serious harm'** is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk

- the level of sensitivity of the personal information accessed, disclosed or lost
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

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 Systems and Processes for Managing a Data Breach

The Commission's Information Security Management System is ISO 27001 2022 certified, providing the Commission with maximum information security, cybersecurity and privacy protection in the event of a data breach. The Commission has established a range of systems, policies and procedures for preventing and managing data breaches.

The Commission's IT network and infrastructure is managed by Experteq and physically located at Macquarie Government Data Centres, who are ISO 27001 certified and who have implemented a number of cyber security measures to mitigate the risk of data breaches.

The Commission will ensure all third-party providers who store personal and health information on behalf of the Commission, are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches to the Commission.

This policy establishes a process for reporting, managing and responding to data breaches including notifications to the Privacy Commissioner and affected individuals. The Policy also includes steps for reviewing, responding, and developing remedies for preventing data breaches.

The Commission also maintains an internal register of data breaches and has implemented recommended changes to systems and policies in response to reviewing the causes of data breaches to assist in preventing future breaches.

Information security and cyber security training is mandatory for all Commission staff and provided regularly. The Commission will continue to review the training needs of staff with respect to data breaches and provide training in the MNDB Scheme, reporting, managing and responding to data breaches.

The Commission has established a Protective Security Framework Risk Register, in accordance with the requirements of ISO 27001, which is reviewed monthly, and includes:

- Information security, cyber security and privacy risks
- Governance security risks
- Personal security risks
- Physical security risks

The risk register captures:

- Risk cause
- Risk impact
- Risk mitigation
- Risk owner

The Commission's ICT Disaster Recovery Plan addresses recovery of ICT systems including disruptions resulting from cyber incidents, in accordance with the requirements of the Business Impact Assessment and the Business Continuity Plan. The Commission also conducts annual cyber security exercises to test the responsiveness of the Business Continuity Plan, Cyber Incident Response Plan and ICT Disaster Recovery Plan, in accordance with the BCM Policy and Procedure, and the requirements of the NSW Cyber Security Policy.

## 7 Reporting and Responding to a Data Breach

The Chief Operating Officer must be informed of any data breach to ensure the application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

There are five key steps required in responding to a data breach:

1. Identify the breach
2. Contain the breach
3. Assess risk and mitigate
4. Notification
5. Review the incident

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Chief Information Officer or their nominee will coordinate with Experteq to address and respond to identified data breaches related to its IT systems.

***Step one: Identify the breach***

A staff member, contractor or third-party provider is to notify the Chief Operating Officer within one business day of becoming aware that a data breach

has occurred and provide information about the type of data breach as detailed in Section 5 of this Policy. The Chief Operating Officer will notify the Commissioner immediately of a suspected eligible data breach. The Privacy Officer will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme, complete the Data Breach Report and Action Plan and include all data breaches in the Commission's Internal Data Breach Register.

Members of the public are also encouraged to report any data breaches to the Commission in writing by using the contact options available on the Commission website. If a data breach occurs as a result of action from Commission ICT and IMT staff the Chief Information Officer will immediately notify the Chief Operating Officer, who will determine whether a Data Breach Response Team will be convened to undertake steps 2-5 in the process of responding to a data breach. The Chief Operating Officer may also consider convening a Data Breach Response Team, where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual.

***Step two: Contain the breach***

Containing the breach is prioritised by the Commission. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the breach, or revoke or change access codes or passwords.

If a third-party is in possession of the data and declines to return it, it may be necessary for the Commission to seek legal or other advice on what action can be taken to recover the data. When recovering data, the Commission will make sure that copies have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third-party that the copy of the data that they received in error, has been permanently deleted.

***Step three: Assess risk and mitigate***

To determine what other steps are needed, the Commission will undertake an assessment of the type of data involved in the breach, whether the breach is an eligible breach under the MNDB Scheme, and the risks and potential for serious harm associated with the breach. The Data Breach Report and Action Plan will be used for reporting on the investigation of the breach and authorising actions in response. The Privacy Officer will prepare a report and provide to the Chief Information Officer who will review the proposed actions and recommendations of the report prior to the Report being provided to the Chief Operating Officer for approval. Data Breach Report and Action Plans are to be saved in Objective, the Commission's electronic record keeping system.

The Chief Operating Officer will be responsible for the implementation of proposed actions and recommendations.

Some types of data are more likely to cause harm if it is compromised. For example, personal information, health information, and security classified information will be more significant than names and email addresses on a newsletter subscription list.

A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- **Who is affected by the breach?** The Commission assessment will include reviewing whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
- **What was the cause of the breach?** The Commission assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Questions include: Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?
- **What is the foreseeable harm to the affected individuals/organisations?** The Commission assessment will include reviewing what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information personal information subject to special restrictions under s.19(1) of the PPIP Act), if could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage the Commission's reputation?
- **Guidance issued by the Privacy Commissioner on assessing eligible data breaches** Upon becoming aware of a possible data breach, the Commission will take into account any guidance issued by the NSW Privacy Commissioner.

In order to mitigate the breach, the Commission will consider the following measures:

- Implementation of additional security measures within the Commission's own systems and processes to limit the potential for misuse of compromised information.
- Limiting the dissemination of breached personal information. For example, by scanning the internet to determine whether the lost or stolen information has been published and seeking its immediate removal from public sites.
- Engaging with relevant third parties to limit the potential for breached personal information to be misused for identity theft or other purposes, or to streamline the re-issue of compromised identity documents. For example, contacting an identity issuer or financial institution to advise caution when relying on particular identity documents for particular cohorts.

***Step four: Notification***

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered. There are four elements of the notification process:

1. Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form.
2. Determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, the Commission may not be required to notify affected individuals.
3. Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
4. Provide further information to the Privacy Commissioner.

The Commission recognises that notification to individuals/organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations. Notification demonstrates a commitment to open and transparent governance, consistent with the Commission's approach. If a data breach is not an eligible data breach under the MNDB Scheme, the Commission may still consider notifying individuals/organisations of the breach dependent upon the type of information that is involved, the risk of harm, repeated and/or systematic issues and the ability of the individual to take further steps to avoid or remedy harm.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Considerations include the following:

#### When to notify

Individuals/organisations affected by a data breach will be notified as soon as practicable. Whilst this policy sets a target of notification within 5 days; practical factors are also recognised. Where all individuals affected by an eligible data breach cannot be notified, the Commission will consider issuing a public notification on its website.

#### How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on the Commission's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). A record of any

public notification of a data breach will be published on the Commission's website and recorded on the Public Data Breach Register for a period of twelve months.

### What to say

Section 590 of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

1. the date the breach occurred
2. a description of the breach
3. how the breach occurred
4. the type of breach that occurred
5. the personal information included in the breach
6. the amount of time the personal information was disclosed for
7. actions that have been taken or are planned to secure the information, or to control and mitigate the harm
8. recommendations about the steps an individual should take in response to the breach
9. information about complaints and reviews of agency conduct
10. the name of the agencies that were subject to the breach
11. contact details for the agency subject to the breach or the nominated person to contact about the breach.

### Other obligations including external engagement or reporting

The Commission will also consider whether notification is required by contract or by other laws or administrative arrangements to take specific steps in response to a data breach. These may include taking specific containment or remediation steps or engaging with or notifying external stakeholders (in addition to the Privacy Commissioner), where a data breach occurs.

Depending on the circumstances of the data breach this could include:

- NSW Police Force and/or Australian Federal Police, where the Commission suspects a data breach is a result of criminal activity
- Experteq, where a data breach could have an impact on the Commission's IT network or could affect the operations or data holdings held by another NSW government agency
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a data breach is a result of a cyber security incident
- The Office of the Australian Information Commissioner, where a data breach may involve agencies under the Federal jurisdiction
- Any third-party organisations or agencies whose data may be affected
- Financial services providers, where a data breach includes an individual's financial information
- Professional associations, regulatory bodies or insurers, where a data

breach may have an impact on these organisations, their functions and their clients

- The Australian Cyber Security Centre where a data breach involves malicious activity from a person or organisation based outside Australia.

***Step five: Review the incident***

The Commission will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Depending on the nature of the breach step five may be completed as part of the assessment of the first four steps and mitigation of the breach as detailed in step three above.

Preventative actions could include a:

- compliance with ISO 27001, which includes selected controls from ISO 27701
- review of the Commission's IT systems and remedial actions to prevent future data breaches
- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

Any recommendations to implement the above preventative actions are to be approved by the Chief Operating Officer and documented in the Commission's Continuous Improvement Log, in accordance with the requirements of ISO 27001 clause 10.1. Consideration will be given to reporting relevant matters to the Commission's Audit and Risk Committee.

## 9 Communications Strategy

The Privacy Officer through the Chief Operating Officer will be responsible for all communications issued under this Policy. The Commission will aim to notify affected individuals, and external reporting agencies within five business days of a data breach of Commission held information being reported to the Commission. Notifications to individuals will have regard for this Policy as well as the Commission's Privacy Management Plan. Where engagement with external reporting authorities is required, the Privacy Officer will consult with the Chief Operations Officer and other Executive Team members as required. The Commission's Business Continuity Plan and ICT Disaster Recovery Plan contain instructions for communication messaging for specific incidents including a cyber security incident.

## 10 Related Legislation, Policies and Procedures

- Business Continuity Plan

- Cyber Incident Response Plan
- Data Breach Response Plan
- Privacy Management Plan
- Security Incident Management Policy and Procedure
- Security Incident Reporting Policy and Procedure
- Risk Management Framework
- Data Breach Register
- ISO 27001 2022 Information security, Cybersecurity and Privacy Protection
- ISO 27701 2019 Extension to 27001 – Privacy Information Management
- Government Information (Public Access) Act 2009
- Health Records and Information Privacy Act 2002
- Privacy and Personal Information Protection Act 2023

## 11 Feedback

Any feedback regarding this policy can be sent to the Privacy Officer.