



NSW Crime Commission Data Breach Response Plan

October 2023

Document Control

This document is only valid on the day it was printed. The source of the document is located in the Business Continuity Management documentation in Objective

Authors

| |
|------------|
| M Livesley |
|------------|

Version History

| Date | Version | Revision History | Author /Reviser |
|--------------|---------|------------------|-----------------|
| October 2023 | V0.1 | Initial draft | PMO |
| | | | |
| | | | |

Document Reviews

| Date | Version | Comments | Reviewed by |
|------|---------|----------|-------------|
| | | | |

Approvals

This document requires the following approvals.

Date of issue and version details must be entered upon approval.

| Name | Title | Date of Issue | Version |
|------------|-------------------------|---------------|---------|
| Mike Wilde | Chief Operating Officer | 22 Nov 2023 | V1.1 |
| | | | |

| | |
|------------------------------------|--|
| Responsible Business Group: | Corporate and Enterprise Services Division |
| Distribution: | Restricted (Business Operations Committee, Data Breach Response Team, Audit and Risk Committee) |
| Security: | <u>PROTECTED</u> |

CONTENTS

| | | |
|------------|--|-----------|
| 1.0 | INTRODUCTION..... | 4 |
| 2.0 | SCOPE..... | 4 |
| 3.0 | DATA BREACH RESPONSE TEAM..... | 4 |
| 3.1 | Communication Responsibilities..... | 4 |
| 4.0 | NSW CRIME COMMISSION RESPONSIBILITIES..... | 5 |
| 5.0 | GOVERNANCE ARRANGEMENTS..... | 5 |
| 5.1 | Review and Update..... | 5 |
| 5.2 | Training..... | 5 |
| 5.3 | Continuous Improvement..... | 5 |
| 5.4 | Security..... | 5 |
| 5.5 | Legislative Framework..... | 6 |
| 6.0 | DATA BREACH RESPONSE PLAN..... | 6 |
| 6.1 | Identify the breach..... | 6 |
| 6.2 | Contain the breach..... | 7 |
| 6.3 | Assess risk and mitigate..... | 7 |
| 6.4 | Notification..... | 8 |
| 6.5 | Review the incident..... | 8 |
| A.0 | ANNEX..... | 10 |
| A.1 | Emergency Services Contact Details..... | 10 |
| A.2 | Situation Update template..... | 11 |
| A.3 | Incident Log template..... | 12 |
| A.4 | Resolution Action Plan template..... | 13 |
| A.5 | Evidence Register template..... | 14 |
| B.0 | ANNEX..... | 15 |
| B.1 | Data Breach Notification Form to Privacy Commissioner..... | 15 |

1.0 INTRODUCTION

Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (PIIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme. The MNDB Scheme requires every NSW public sector agency bound by the PIIP 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 document, the Data Breach Response Plan (DBRP), supports the Data Breach Policy and defines the steps and procedures to be undertaken in the event of a data breach.

This document has been developed in alignment with the requirements of the PIIP Act, the ISO 27001 standard and the Protective Security Policy Framework.

2.0 SCOPE

This Plan applies across all Divisions, business units and controlled entities of the Commission. It defines the responses and procedures to be applied by the Commission's Data Breach Response Team (DBRT) across the entire organisation.

3.0 DATA BREACH RESPONSE TEAM

The Commission's Data Breach Response Team (DBRT) is responsible for managing responses to data breaches. The DBRT reports to the Chief Operating Officer. The following table provides information on the Commission's DBRT.

| Title | Role | Contact |
|------------------------------------|-------------|---------|
| CIO | ▪ DBRT Lead | |
| PMO & ICT Compliance Manager | ▪ DBRT SME | |
| Privacy Officer | ▪ DBRT SME | |
| Governance Audit & Risk Manager | ▪ DBRT SME | |
| | ▪ | |

3.1 Communication Responsibilities

The Chief Operating Officer and Privacy Officer are responsible for all communications and timely status updates to the Executive Team.

The Executive Team is responsible for passing all information received from the Chief Operating Officer and Privacy Officer to their staff. Executive Directors and Managers **MUST** maintain up to date contact details for their staff to ensure the timely delivery of messages. This includes mobile phone number and personal email address for each staff member.

4.0 NSW CRIME COMMISSION RESPONSIBILITIES

NSW Crime Commission is responsible for the operational response to data breaches affecting Commission systems or services. The Commission is mandated to report all data breaches to the Office of the Information and Privacy Commissioner (IPC) in accordance with the requirements of the PPIP Act.

IPC will work with the Australian Government and other jurisdictions to coordinate information sharing, decision making, and communication.

5.0 GOVERNANCE ARRANGEMENTS

5.1 Review and Update

The Commission's Data Breach Policy requires that the DTRP shall be updated each year or following any significant change to business process or threat profile, to ensure that it remains up to date and effective.

This Plan shall be reviewed and updated, and records of those updates shall be retained, in accordance with the requirements of the DBP.

5.2 Training

The Commission's Data Breach Policy requires that all staff have a role to play in the identification of a data breach and reporting process and shall be trained in relevant procedures. Such staff shall receive training updates each year or following any significant change to those procedures. Training records shall be retained so as to provide an audit trail.

Each member of the Commission's DBRT listed at Clause 4.0 shall receive relevant training in their roles and responsibilities regarding the data breach response process in accordance with the requirements of the DBP.

5.3 Continuous Improvement

The Commission's Data Breach Policy requires that a review is undertaken and documented at the first reasonable opportunity following an actual data breach incident. The review shall be used as an input to the continual improvement process to ensure that opportunities for improvement identified during an actual data breach are noted and captured in the Commission's Continuous Improvement Log

This Plan shall be continually improved, and records of those improvements shall be retained, in accordance with the requirements of ISO 27001 2022 clause 10.1.

5.4 Security

This Plan has been assigned a classification of PROTECTED and shall be labelled, handled and protected in accordance with the requirements defined within the Commission's Information Security Policy.

5.5 Legislative Framework

The Commission's Data Breach Response Plan shall continue to operate in alignment with the DBP and the PPIP Act as well as relevant NSW and Commonwealth legislation.

6.0 DATA BREACH RESPONSE PLAN

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a human resources adviser.

The diagram below identifies five key steps in responding to a data breach. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.



6.1 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 the Data Breach Policy. Information to be provided includes the following:

- the time and date the suspected breach was discovered,

- the type of personal information involved,
- the cause and extent of the breach, and
- the context of the affected information and the breach.

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.

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.

6.2 Contain the breach

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.

6.3 Assess risk and mitigate

The Privacy Officer reporting to the Chief Operating Officer 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 Privacy Officer will prepare a data breach report and action plan 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.

The report and action plan will be used for reporting on the investigation of the breach and authorising actions in response.

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

6.4 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:

- 6.4.1 Notify the Privacy Commissioner immediately after an eligible data breach is identified using the approved form – see Annex B.1.
- 6.4.2 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.
- 6.4.3 Notify individuals: Unless an exemption applies, notify affected individuals or their authorised representative as soon as reasonably practicable.
- 6.4.4 Provide further information to the Privacy Commissioner.

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.

Where all individuals affected by an eligible data breach cannot be notified, the Commission will consider issuing public notification on its website.

6.5 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

It is important to consider that, in some circumstances, a response plan may include the finalisation of a related criminal investigation (including forensic evidence collection), which may need to occur before recovery is possible.

It is essential to obtain legal advice on collecting and preserving evidence in the event of litigation against the Commission resulting from the breach.

Learning from each data breach enables the Commission to continually improve its processes and procedures for managing cyber incidents.

The DBRT (and CRT, if BCP has been activated) should come together for a Post Incident Review to discuss:

- Exactly what happened, and at what times?

- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the response?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organisations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

The discussion should be documented and any key insights / lessons learnt shared with all parties involved. Any recommendations to arise from the discussion should be documented in a corresponding action plan that states how the recommendation will be actioned, by whom and when.

This Data Breach Response Plan will be continually updated to reflect better practice in data breach response activities, including following any relevant post incident reviews.

A.0 ANNEX**A.1 Emergency Services Contact Details**

The following is a list of emergency services to be contacted, as required:

| Entity | Contact |
|---|----------------|
| Fire Brigades | 000 |
| Ambulance | 000 |
| Police – Emergency | 000 |
| Poisons Information Hotline | 13 11 26 |
| Hospital – St Vincent's Darlinghurst Emergency Department | 02 8382 1111 |
| Sydney Hospital Emergency | 9382 7111 |
| Electricity (Ausgrid) | 13 13 88 |
| Gas (AGL Energy) | 13 12 45 |
| Water (Sydney Water) | 13 20 92 |

A.2 Situation Update template

| SITUATION UPDATE: | Update Number: | Date and time: | Author: |
|-----------------------------------|---|----------------|---------|
| | | | |
| DATE AND TIME INCIDENT DETECTED: | | | |
| CURRENT STATUS: | New / In Progress / Resolved | | |
| INCIDENT TYPE: | | | |
| INCIDENT CLASSIFICATION: | Incident / Significant Incident / Emergency | | |
| SCOPE: | list the affected networks, systems and/or applications; highlight any change to scope since the previous log entry | | |
| IMPACT: | list the affected stakeholder(s); highlight any change in impact since the previous log entry | | |
| SEVERITY: | outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry | | |
| NOTIFICATIONS ACTIONED/PENDING: | | | |
| ADDITIONAL NOTES: | | | |
| INCIDENT MANAGER CONTACT DETAILS: | | | |
| DATE AND TIME OF NEXT UPDATE: | | | |



A.3 Incident Log template

| DATE / TIME | NOTES (log, Record facts, decisions and rationale) |
|-------------|--|
| Start time | Start of Incident |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |



A.4 Resolution Action Plan template

| DATE AND TIME | CATEGORY (Contain / Eradicate / Recover / Communications) | ACTION | ACTION OWNER | STATUS (Unallocated / In Progress / Closed) |
|----------------------|---|---------------|---------------------|--|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |




A.5 Evidence Register template

| DATE, TIME AND LOCATION OF COLLECTION | COLLECTED BY (name, title, contact and phone number) | ITEM DETAILS (quantity, serial number, model number, hostname, media access control (mac) address, and IP addresses) | STORAGE LOCATION AND LABEL NUMBER | ACCESS (date, time, person and rationale for access after collection) |
|--|--|--|--|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

B.0 ANNEX

B.1 Data Breach Notification Form to Privacy Commissioner



information and privacy commission
new south wales

Mandatory Data Breach Reporting Form July 2023

Data Breach Notification to the Privacy Commissioner

Section 59M of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires the head of a public sector agency to immediately notify the Privacy Commissioner of an eligible data breach using an approved form. This form has been approved by the Privacy Commissioner for use by agencies for the purpose of notification under section 59M of the PPIP Act.

This approved form sets out the information that agencies must supply to the Privacy Commissioner when making a notification of an eligible data breach, unless it is not reasonably practicable to provide that information.

This document is not to be used for agency's notification to individuals affected by a breach, however the information supplied may be of use when developing your agency's written notification as required by section 59N of the PPIP Act.

Agency making notification

Agency name:

Agency address:

Telephone number:

Contact name:

Contact telephone:

Contact email:

Contact role/title in organisation:

Notification made on behalf of another agency/agencies (if applicable)

Is the notification made on behalf of another agency/agencies? Yes No

If yes, complete the agency details below:

Name:

Address:

Telephone number:

Contact name:

Contact telephone:

Contact role/title in organisation:

If the notification is made on behalf of more than one agency, please provide the above details for each agency as a separate attachment.

Information and Privacy Commission NSW 1
www.ipc.nsw.gov.au | 1800 IPC NSW (1800 472 679)

Data Breach Notification

Form

Type of personal information that was the subject of the breach

Select the option(s) that best apply:

- Contact details
- Identity documents/credentials
- Financial information
- Health information
- Under review (agency is still conducting its assessment at time of notification)
- Other sensitive information:

Description of eligible data breach

Discovery of the breach

- When the data breach occurred:
- When the data breach was discovered:
- Where the data breach was discovered:
- How the data breach was discovered:
- By whom was the data breach discovered:
- Amount of time the personal information was exposed:

Type of breach

Select the type(s) of data breach as applicable:

- Unauthorised disclosure
- Unauthorised access
- Loss of information
- Other:

How the breach occurred

Provide a brief explanation as to how the breach occurred:

Cause of breach

- Cyber Incident

If the breach was caused by a Cyber Incident, select the type of Cyber Incident below:

Data Breach Notification

Form

Ransomware

Malware

Phishing (compromised credentials)

Compromised credentials (method unknown)

Hacking

Brute Force Attack (compromised credential)

Other: _____

Human Error

Loss/theft of data/equipment

System fault

Other: _____

Remedial action taken to date (including description of action and when)

Remedial action to be taken

Notification to affected persons

Total number of individuals affected, or likely to be affected by the breach (provide best estimate if exact figure is unknown): _____

Total number of individuals notified of the breach at this stage: _____

Total number of individuals yet to be notified of the breach: _____

Provide details of how and when individuals were notified: _____

Have individuals been advised of the complaints and internal review procedures under the PPIP Act?

Recommendations made to affected individuals about the steps they should take to mitigate the effects of the breach

Estimated cost

Estimated cost of the breach to the agency: _____

Other bodies notified



Data Breach Notification

Form

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

B.1 Data Breach Notification Form to Privacy Commissioner**Step 1: Identify the breach (Commission staff)**

Record and advise Chief Operating Officer of the following:

- the time and date the suspected breach was discovered
- the type of personal information involved
- the type of personal information involved
- the context of the affected information and the breach.

Step 2: Contain the breach (Privacy Officer)

- Understand and assess the data breach, or suspected data breach.
- Co-ordinate any action required to contain the data breach.
- Notify the Chief Privacy Officer (Chief Operating Officer) about the data breach, details of the breach and recommended actions.

Step 3: Assess the risks and mitigate (Privacy Officer)

- Conduct investigation to establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Notify through the Chief Operating Officer the Executive.
- Keep appropriate records of the suspected breach including any action taken.

Step 4: Notification (Privacy Officer through the Chief Operating Officer)

- Determine who needs to be made aware of the breach at this stage.
- Determine whether and how to notify affected individuals.
- Determine whether to escalate the data breach to the response team.
- Convene the response team, if necessary.
- Determine whether the breach is an eligible data breach under the NDB scheme.
- Notify the AIC of the NDB, if necessary.

Step 4: Review the incident (Data Breach Response Team)

- Fully investigate the cause of the breach.
- Implement a strategy to identify and address any weaknesses in NSWCC data handling.
- Conduct a post-breach review and report to the Chief Operating Officer on outcomes and recommendations.
- Update Data Breach Response Plan if required.