Data Breach Policy

Contents

1. Data Breach Policy

1.1 Purpose

This Policy sets out the framework for responding to a breach of data held by the Public Service Commission (PSC) and our procedures for compliance with Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

Part 6A of the PPIP Act creates the Mandatory Notification of Data Breach Scheme (MNDB Scheme). The MNDB Scheme requires NSW public sector agencies to notify the Privacy Commissioner and affected individuals of certain data breaches known as Eligible Data Breaches, and to prepare and publish a Data Breach Policy for managing such breaches. The MNDB Scheme also requires that NSW public sector agencies must establish and maintain an internal register and a public notification register of Eligible Data Breaches.

Having effective data breach management procedures allows the PSC to respond quickly to a data breach, and reduce or avoid harm to affected individuals, organisations and the PSC, and may prevent future breaches.

1.1. Scope

This policy provides guidance to PSC staff on actions and responsibilities in the event of a data breach, including:

- what constitutes an Eligible Data Breach under the PPIP Act
- roles and responsibilities of PSC staff in the event of a data breach,
- the steps involved in responding to an Eligible Data Breach
- review and evaluation of systems, policies and procedures to prevent future data breaches.

This policy applies to all staff and contractors of the PSC. This includes temporary and casual employees, volunteers, private contractors and consultants engaged by the PSC 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 PSC.

1.2. Legislative and policy context

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)
- *Privacy Act 1988* (Commonwealth)
- *Data Sharing (Government Sector) Act 2015* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)

- PSC Privacy Code of Practice
- PSC Health Privacy Code of Practice

- PSC Privacy Management Plan
- PSC Information Security Management System Policy and Incident Management Policy.
- PSC Business Continuity Plan.

1.3. Related resources

See Information and Privacy Commission website for Privacy Commissioner's guidelines, approved forms, resources and further information about the MNDB Scheme at https://www.ipc.nsw.gov.au/privacy/MNDB-scheme.

1.4. Roles and responsibilities

The Public Service Commissioner has overall responsibility for compliance with the MNDB scheme. The Commissioner has responsibility for exercising or delegating the exercise of functions allocated to agency heads under the PPIP Act:

- Receive reports of any suspected Eligible Data Breach (section 59E)
- Make all reasonable efforts to contain the data breach and within 30 days carry out an assessment of whether the data breach is, or there are reasonable grounds to believe the data breach is, an Eligible Data Breach (section 59E)
- During a data breach assessment, make all reasonable attempts to mitigate harm done by the suspected breach (section 59F)
- Direct one or more persons to carry out and complete data breach assessments within 30 days of report (section 59G)
- Receive the assessor's advice as to whether, a data breach is an Eligible Data Breach or there are reasons to believe a data breach is an Eligible Data Breach (section 59J)
- Decide whether, a data breach is an eligible data breach or there are reasons to believe a data breach is an Eligible Data Breach (section 59J)
- Approve an extension of time for a data breach assessment and notifying the Privacy Commissioner of such approval and the relevant extension period (section 59K)
- If the Public Service Commissioner decides that an eligible breach has occurred or that there are reasonable grounds to believe the data breach is an Eligible Data Breach:
    - immediately notify the Privacy Commissioner in the approved form of an Eligible Data Breach (section 59M) and any further information (section 59Q)
    - take reasonable steps to notify each individual to whom the personal information the subject of the breach relates and each affected individual (section 59N, 59O)
    - publish a notification on the PSC's public notification register (section 59P)
    - decide to exempt the PSC from Division 3, Subdivision 3 of the PPIP Act and notify the Privacy Commissioner of such exemption (section 59W, 59X)
    - provide a statement to the Privacy Commissioner in response to a direction to prepare a suspected Eligible Data Breach (section 59Y)
    - make a submission to the Privacy Commissioner (section 59ZC)
- Prepare and publish a data breach policy (section 59ZD)

- Establish an internal register for Eligible Data Breaches (section 59ZE).

The Associate Director, ICT & Business Services (Chief Information Security Officer, CISO) is responsible for:

- Implementing this Policy,
- Receiving reports of suspected data breaches from PSC staff, contractors or third-party providers
- Reporting data breaches to the Public Service Commissioner, including all notifications, preparation of data breach assessment report and recommended actions in relation to Eligible Data Breaches,
- Assessing and responding to suspected data breaches in accordance with this Policy Coordinating consultation with internal and external stakeholders
- Notifying Eligible Data Breaches to Privacy Commissioner and other relevant authorities as required
- Providing information to the Director Governance and Risk/CFO for inclusion in the PSC's internal register of Eligible Data Breaches and public notification register
- Conducting an annual review of breach response records
- Performing any of the Commissioner's functions which the CISO is authorised or required to perform (whether under this Policy or the Information Security Policy (ISMS) or otherwise) or which are delegated to the CISO
- Training staff in data breach management and reporting
- The CISO forms part of the Security Incident Response Team (**SIRT**).

The Chief Risk Officer (CRO) is responsible for:

- Overseeing and promoting sound risk management practices pertaining to this Policy and within the PSC generally,
- Identifying and analysing emerging data breach risks across the PSC and reporting these to relevant stakeholders,
- Providing objective challenge to Risk Owners regarding day-to-day management of data breach risks, and completeness and accuracy of risk information and data,

and forms part of the SIRT.

The Director Governance and Risk/CFO is responsible for:

- Embedding data breach risk management practices in the day-to-day operations of the PSC,
- Leading the SIRT
- Maintaining the PSC's internal register of Eligible Data Breaches and public notification register
- Ensuring timely reporting of any data breach risks to the Public Service Commissioner, CISO and CRO, and forms part of the SIRT.

The Associate Director, Strategic Communications is responsible for advising in relation to the communication strategy and messaging to affected individuals and external reporting agencies, and forms part of the SIRT.

General Counsel is responsible for managing the provision of legal advice in relation to issues arising under this policy, and forms part of the SIRT.

The Chief Audit Executive (CAE) is responsible for:

Monitoring and reporting to the PSC and PSC's Audit and Risk Committee in relation to the application of this Policy and implementation of any agreed action plans following an Eligible Data Breach, and forms part of the SIRT.

All PSC staff are required to:

- Immediately report any suspected Eligible Data Breach to the Public Service Commissioner and the Chief Information Security Officer (CISO) if they become aware that a data breach has occurred or suspect that a data breach may have occurred, and provide information about the data breach; andUndertake mandatory cybersecurity training once per year, and refresher courses as they come up during the year.

2. What is an Eligible Data Breach?

Under the PPIP Act, the PSC has certain obligations under the MNDB Scheme if there is an **Eligible Data Breach.** An Eligible Data Breach occurs where:

1. there is an unauthorised access to, or unauthorised disclosure of, **personal information** held by the PSC, or there is a loss of personal information held by the PSC 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 to, or disclosure of, the information would be **likely to result in serious harm** to an individual to whom the information relates.

An Eligible Data Breach may involve disclosure within the PSC, or between the PSC and another government sector agency, or by an external person or entity accessing data held by the PSC without authorisation.

An Eligible Data Breach may involve human error, system failure and/or malicious or criminal attack.

Personal information

For the purposes of this policy and MNDB Scheme, a reference to '**personal information'** includes 'personal information as defined in the PPIP Act and 'health information' as defined in the HRIP Act unless otherwise indicated.

The PPIP Act defines 'personal information' as: *"information or an opinion (including information or an opinion forming part of a database and whether or not recorded in material form) about whose identity is apparent or can reasonably be ascertained from the information or opinion"* (section 4 PPIP Act). This could include details such as an individual's name, address, phone number, email address, date of birth and tax file number. There are some exclusions from the definition of 'personal information' set out in section 4(3) of the PPIP Act.

The HRIP Act defines 'health information' (relevantly to the PSC) as: *"personal information that is information or an opinion about … the physical or mental health or a disability (at any time) of an individual"*. There is a more detailed definition of 'health information', including some exclusions, in section 6 of the HRIP Act.

Serious harm involves real and substantial detrimental effect to the individual, not mere irritation, annoyance or inconvenience. Whether access to or disclosure of personal information is likely to result in serious harm to the individual will depend on the context. Factors to consider in determining whether a data breach is likely to result in serious harm are set out in **Appendix C**.

- the type of personal information accessed, disclosed or lost and whether a combination of types of personal information may 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
- the circumstances of the individuals concerned and their vulnerability or susceptibility to harm
- the circumstances in which the breach occurred, and
- actions taken to reduce the risk of harm following the breach.

Harm may include physical harm; economic, financial or material harm; emotional or psychological harm; and other forms of serious harm that a reasonable person in the PSC's position would identify as a possible outcome of the data breach.

Examples of data breach

Examples of data breaches include:

- Accidental loss or theft of NSW Government confidential material or equipment on which such data is stored (e.g. a paper record, laptop, mobile phone, USB Stick)
- Unauthorised use, access to or modification of data or information systems (e.g., sharing official login details (deliberately or accidentally) to allow another to gain access or make unauthorised changes to PSC's data or information systems)
- Unauthorised disclosure of personal information (e.g. accidentally sending an email to an incorrect recipient, posting official documents to an incorrect address, posting third-party information on the PSC website or social media channels without consent)
- Compromised user account (e.g. accidentally disclosing user login details through phishing)
- System and process failure
- Spear phishing (a targeted attempt to steal sensitive information from a specific person)
- Malware infection
- Ransomware attack.

There may be some overlap between information security incidents and Eligible Data Breaches, but they are not the same thing. Some cybersecurity incidents will not impact anyone's personal and health information, and so they will not be an Eligible Data Breach. However, information security incidents may constitute an Eligible Data Breach where there has been a disclosure of or accidental loss or theft of personal information or equipment on which such data is stored.

Certain types of data breaches are more likely to cause harm if the information has been compromised. For example, a data breach involving sensitive personal information, health information, information subject to legal professional privilege and/or NSW Government Cabinet information is more likely to cause harm. In contrast, a data breach containing basic personal information already in the public domain is less likely to result in serious harm.

3. Responding to a data breach

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

1. Initial report and triage
2. Contain the breach
3. Assess and mitigate
4. Notify
5. Review and prevention.

All steps other than “Review” should be carried out concurrently where possible. The “Review” step provides recommendations for longer-term solutions and prevention strategies.

3.1 Initial report and triage

PSC staff, contractors or third-party providers must notify the PSC’s Chief Information Security Officer (CISO) immediately or within 24 hours of becoming aware that a data breach has occurred, and provide as much information as possible about the type of data breach.

Members of the public are encouraged to report any data breaches involving PSC held data to the PSC in writing by using the Contact Us details on our website.

The CISO will triage by conducting preliminary fact finding and initial assessment as set out in Steps 2-3 to form an initial view as to whether the breach is Low, Medium or High Risk, and whether it is or may be an Eligible Data Breach under the MNDB Scheme.

The CISO will notify the Public Service Commissioner of any suspected Eligible Data Breach or other High Risk breach.

The Public Service Commissioner will determine whether a Security Incident Response Team (SIRT) will be convened (or expanded if a SIRT has already been convened) to undertake steps 2 – 5 in responding to the suspected Eligible Data Breach. The SIRT convened for the purposes of this Policy will comprise of the CISO, Chief Risk Officer, Director Governance and Risk/CFO, Chief Audit Executive (CAE), Associate Director Strategic Communications, General Counsel and other appropriate staff, depending on the circumstances of the breach.

The CISO will work quickly and effectively with the SIRT (if convened) to respond to the breach.

The CISO will coordinate consultation with the:

- Government Chief Information Security Officer,
- Cyber Security NSW,
- ID Support NSW,
- GovConnect,
- Department of Customer Service and/or its service providers, and
- Premier’s Department.

3.2. Contain the breach

Containing any data breach is prioritised by the PSC.

The SIRT and CISO must immediately make all reasonable efforts to contain the breach and minimise resulting damage. Steps taken to contain the breach should be documented.

The CISO will lead breach containment in consultation with the SIRT and relevant external agencies.

Steps may include, for example:

- Searching for and recovering breached data,
- Shutting down breached computer systems,
- Suspending the activity that led to the breach,
- Confirming if any personal information was included in the breached data,
- Confirming whether any copies were made of breached data,
- Ensuring that the breached data and any copies are destroyed or returned by the party receiving it. (If the third party declines to destroy or return the data, it may be necessary to seek legal advice about what actions can be taken to recover the data)
- Wiping a lost portable device,
- Revoking access to systems from specified users,
- Changing usernames and passwords,
- Contacting third party vendors/suppliers if the breach also involves them.

To inform containment work, the PSC will conduct **preliminary fact-finding research** about the breach to discover:

- The cause,
- Nature of the information involved in the breach,
- Options to mitigate the breach and further impacts,
- Risk of the breach spreading,
- Number and location of the individuals or organisations affected by the breach,
- Any other relevant information about the individuals or organisations affected, including whether they are experiencing vulnerability, or whether the breaching party had malicious intent.

3.3. Assess and mitigate

Assessment of breach

The PSC must carry out an assessment of the breach to determine:

- the type of data involved in the breach
- what other steps are needed to respond to the breach, whether the breach is **an Eligible Data Breach** or there are reasonable grounds to believe the data breach is an Eligible Data Breach, and
- the risks and potential for serious harm associated with the breach.

The data breach assessment must be conducted in an expeditious way within 30 days (or such extended period approved by the Commissioner).

The data breach assessment is to be conducted by the CISO in consultation with the SIRT (if convened) in accordance with this Policy, the requirements of the PPIP Act and any applicable guidelines issued by the Privacy Commissioner.

Factors that PSC may consider in carrying out the data breach assessment include those set out in section 59H of the PIPP Act and below:

- **The personal information involved in the breach?**
  - What types of personal information were involved in the breach? (personal, health, encrypted etc.)
  - The sensitivity of the personal information involved in the breach?
  - Whether the personal information is or was protected by security measures?
- **Who is affected by the breach?**
  - Which individuals and/or organisations have been affected by the breach, and who may be affected by the breach in the future.
  - Whether those individuals whose information is compromised have personal circumstances that would put them at a greater risk of harm.
- **What caused the breach?**
  - The circumstances of the breach, including whether it was a targeted attack, an accident caused by negligence, or a mistake.
  - Whether the breach has occurred previously or not, whether it is a on-off incident, and whether it exposes any systemic vulnerability.
- **What is the foreseeable harm to affected individuals and organisations?**
  - Who has received or could receive unauthorised access to/unauthorised disclosure of the data? What is the risk of further access, use or disclosure via media or online?
  - The likelihood of recipients of breached data causing harm or circumventing security measures protecting the information.
  - The nature of the harm that has occurred or may occur. How a recipient of breached data may use the data, e.g. for identity theft, or to damage an individual's or the PSC's reputation.
  - The **seriousness** of the harm to one or more individuals whose information is involved in the breach. Factors to consider in determining the likelihood of **serious harm** are set out in section 2 and **Appendix C.**
- **Guidance issued by the Privacy Commissioner on assessing Eligible Data Breaches.**

Data breach assessment report

The CISO will prepare a data breach assessment report and action plan in the form of **Appendix B.**

The CISO will advise the Commissioner whether the assessment found that the data breach is an **Eligible Data Breach** or there are reasonable grounds to believe the data breach is an Eligible Data Breach.

The Commissioner will then decide whether the breach is an **Eligible Data Breach** or there are reasonable grounds to believe the data breach is an Eligible Data Breach.

Mitigation

The PSC must take all reasonable attempts as soon as practicable to prevent or lessen the likelihood of harm the breach may pose to individuals or organisations.

In order to mitigate the breach, the PSC may consider the following measures:

- Implementation of additional security measures 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.
- Providing staff with instructions on any immediate action that needs to be taken by them, e.g. not clicking attachments or links in emails.

Consultation

For all Low and Medium Risk breaches, the CISO will work with the impacted area and Information Asset Owner/s, General Counsel and any necessary specialists to determine and implement the remaining steps in the data breach response process in consultation with the SIRT.

For High Risk breaches, the CISO will notify the SIRT immediately to oversee the assessment, mitigation and remaining steps in the data breach response process in consultation with the SIRT.

3.4. Notify

3.4.1 When is notification mandatory?

The PSC is required by **law** to notify the Privacy Commissioner and relevant individuals of certain data breaches. Key current requirements are summarised below.

Notification of Eligible Data Breach under NSW PPIP Act

Under the NSW Mandatory Notification of Data Breach (MNDB) Scheme, notification of data breach is required where:

- Personal information and/or health information is involved, *and*
- The assessment has shown there are reasonable grounds to believe that the breach will cause **serious harm** (or likely cause **serious harm**) to one or more individuals. This is a High Risk breach, *and*

- The Commissioner decides that an **Eligible Data Breach** has occurred, or that there are reasonable grounds to believe the data breach is an Eligible Data Breach.

In these circumstances, the Commissioner (or an authorised delegate) must:

1. immediately notify the NSW Privacy Commissioner in the approved form of the Eligible Data Breach (see Section 3.4.2 below);
2. determine whether the PSC is required to notify individuals of the Eligible Data Breach or whether an exemption to notification applies under the PPIP Act[1]; and
3. if required and to the extent reasonably practicable, take reasonable steps to promptly notify relevant individuals and/or publish a notification in accordance with the PPIP Act.
4. provide further information to the Privacy Commissioner as required by the PPIP Act.
5. add the Eligible Data Breach to the PSC's internal register of Eligible Data Breaches as required by section 59ZE of the PPIP Act.
6. add the Eligible Data Breach to the PSC's public notification register on its website if required by section 59P of the PPIP Act.

Notification of data breaches involving TFNs under Cth Privacy Act

Under the Commonwealth Notifiable Data Breaches (NDB) scheme, the PSC must notify the Australian Information Commissioner of a breach if:

- PSC collects Tax File Numbers (TFNs) and the data breach involves a TFN, *and*

[1] See sections 59S – 59X of the PPIP Act and Information and Privacy Commission guidance on exemptions from notification available at: https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements

- The assessment has shown there are reasonable grounds to believe that the breach will cause **serious harm** (or likely cause **serious harm**) to one or more individuals.[2] This is a High Risk breach.

Data breach notification under NSW Data Sharing (Government Sector) Act 2015

Under the *Data Sharing (Government Sector) Act 2015* (NSW) (DSGS Act), the PSC must notify of a breach of data containing personal information or health information shared under that Act if:

- The data involved was received from another government sector agency (as defined in the Act) or the NSW Data Analytics Centre, *and*
- Privacy legislation has been (or is likely to have been) breached in relation to the data while it was in PSC's control.

In this case, the PSC has a mandatory duty to inform the data provider (ie, the government sector agency from which the PSC received the data) and the NSW Privacy Commissioner as soon as is practicable after becoming aware of the breach. Informing the affected individuals is voluntary.

Other notification requirements

The PSC will consider whether any additional notification requirements apply to the PSC in the specific circumstances of the breach, for example under any other legislation, by contract or under other administrative arrangements.

The CISO will coordinate notification, updates/reporting to and/or consultation with relevant internal or external parties. External parties may include:

External parties:
- Government Chief Information Security Officer (CISO)
- Cyber Security NSW
- ID Support NSW
- NSW Privacy Commissioner
- NSW Police Force and/or other law enforcement agencies
- NSW Treasury Managed Fund
- Australian Cyber Security Centre
- Office of the Australian Information Commissioner
- Australian Federal Police
- Australian Taxation Office
- IDCARE and/or the National Identify and Cyber Support Service (if there is a risk that the personal information exposed in the breach could be used for identity theft or other types of fraud).

[2] See Information and Privacy Commission's Fact Sheet – NSW public sector agencies and data breaches involving tax file numbers, updated July 2022, available at https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-data-breaches-involving-tax-file-numbers.

- Professional or other regulated bodies, credit card companies, financial institutions, credit reporting agencies, third-party contractors, or groups representing affected individuals.

3.4.2 How to make mandatory notifications

Required format for notification of Eligible Data Breach under NSW PPIP Act

If notifying an Eligible Data Breach under the PPIP Act, the CISO will take the following steps.

1. Fill out the Information and Privacy Commission's Data Breach Notification to the Privacy Commissioner form[3]. The form should be completed by copying relevant information from the Data Breach Response Report (**Appendix A**) approved by the Commissioner under step 3 (Assess and Mitigate). See **Appendix C** for the information that is required to be reported under s 59M of the PPIP Act.

2. Send the form to the NSW Privacy Commissioner (NSW IPC) immediately via email at ipcinfo@ipc.nsw.gov.au.

Unless the Commissioner has determined that an exemption applies or the PSC is not required to notify, the PSC will then take the following steps in consultation with relevant law enforcement agencies and Cyber Security NSW:

3. Notify relevant individuals or organisations directly (by telephone, letter, email or both in person and in writing) and as soon as practicable. Section 59O of the PIPP sets out the information which must, if reasonably practicable, be included in the notification (see list at **Appendix C**).

4. If the PSC is unable to notify, or if it is not reasonably practicable for it to notify, any or all of the individuals of the Eligible Data Breach, then it may decide to notify individuals indirectly – for example, by information on the PSC's website or a media release.

   This type of indirect notification should generally only occur where the PSC does not have the contact information of affected individuals or organisations, or where direct notification will be prohibitively expensive or cause further harm.

5. A record of any public notification of a data breach will be published on the PSC's website and record on the PSC's public data breach register for a period of 12 months. The information on the register should not include personal information or information which would prejudice the PSC's functions.

[3] See https://www.ipc.nsw.gov.au/sites/default/files/2023-10/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf.

6. As soon as practicable after such notification is published, the PSC will notify the Privacy Commissioner with information about how to access the notification on the public notification register (for example, a link to the PSC's website where the register is kept).

7. Records will be kept as set out in Section 1.10 (Record Keeping) below.

Required format for notification of data breaches involving TFNs

If notifying a High Risk breach involving TFNs, the CISO will take the following steps:

1. Fill out the Office of the Australian Information Commissioner (OAIC) Notifiable Data Breach electronic form. The form should be completed by copying relevant information from the Data Breach Response Report (**Appendix B**) approved by the Commissioner under step 3 (Assess and Mitigate).
3. This form will be sent automatically to the Australian Privacy Commissioner.

Required format for notification under DSGS Act

If the data breach involves information received under the DSGS Act, the CISO will take the following steps:

1. Write a statement and provide it to the data provider *and* the NSW Privacy Commissioner via email at ipcinfo@ipc.nsw.gov.au as soon as practicable.

2. The statement will also be provided directly to affected individuals as soon as practicable.

When to notify

Notification should be undertaken promptly to help avoid or lessen damage by enabling individuals/organisations to take steps to protect themselves.

- **NOTE:** In all cases, the PSC must first consult with any appropriate law enforcement agencies or police investigating the breach before making details of the breach public or providing a statement to the public.

There could, for example, be an exception to notifying an individual, e.g. the notification would interfere with a court proceeding, breach a secrecy provision, or create a further serious risk of harm.[4]

If the breach involves a contracted service provider, other agency, or NGO, a joint notification will be made on behalf of all the organisations involved. This notification will be made by the

[4] See sections 59S through 59X of the PPIP Act, and guidance from the IPC at https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements.

PSC unless breach notification is being led by another agency.[5] If another agency is leading the investigation and notification process, the PSC will follow that agency's notification procedure so far as applicable.

3.5. Review and prevention

- For **all** breaches, the PSC will conduct a review to determine all relevant causes and consider what measures could be taken to prevent any reoccurrence. Preventative actions could include:
    - A security audit,
    - Modifications to physical controls such as locks, alarms, and visitor access controls,
    - A review of policies and procedures,
    - A review of employee training and selection practices,
    - A review of suppliers and third parties, including relevant contractual obligations,
    - Updating passwords, *and*
    - Altering technology deployments.
- For **High and Medium Risk** Breaches, the CISO will submit a report within ten (10) working days to the SIRT outlining the organisational response and mitigation plan.
- For **Low and Medium Risk** Breaches, the CISO will propose recommendations to implement preventative actions and any amendments to the process in responding to future breaches.

The CISO will brief the Public Service Commissioner in relation to any recommendations arising out of the review for the Commissioner's approval and documentation in the PSC's official records management system. Consideration will be given to reporting relevant matters to the PSC's Audit and Risk Committee.

3.6. Record keeping

Appropriate records will be maintained to provide evidence of how suspected and actual breaches are managed. This allows PSC to monitor, analyse, and review the type and severity of suspected and actual breaches.

The PSC will establish and maintain an internal register for Eligible Data Breaches in accordance with its obligations under section 59ZE of the PPIP Act. The register must include, where practicable, the following details:

(a) who was notified of the breach,
(b) when the breach was notified,
(c) the type of breach,
(d) details of steps taken by the public sector agency to mitigate harm done by the breach,

[5] The notifiable data breach scheme applies if the data involved in the breach was held directly by our agency, or if it was held on our behalf by a contracted service provider such that our agency was still in 'control' of the data; see s.59C of the PPIP Act, compared with s.4(4).

(e) details of the actions taken to prevent future breaches,
(f) the estimated cost of the breach.

Where relevant, the PSC will keep a public data breach register on the PSC's website in accordance with its obligations under section 59P of the PPIP Act.

The Director Governance and Risk/CFO will keep and maintain the internal register and public data breach register, and conduct an annual review of breach response records to identify and remedy:

- Weaknesses in security or processes that are prone to error, and
- Any deficiencies in PSC's response policy that impact on its effectiveness.

4. Communicating about data breaches

The Associate Director, Strategic Communications will be responsible for all communications to the public or the media issued under this Policy.

Communications will have regard to this Policy, the PSC's Privacy Management Plan and other applicable policies.

The PSC Strategic Communications Team will develop a proactive strategy for supporting the Associate Director, ICT & Business Services and the SIRT to prepare information and FAQs for internal and external audiences.

Communication to PSC staff will include instructions not to comment publicly or privately (including on social media) about the breach, and that any media communications must be handled by the Associate Director, Strategic Communications.

5. Document information

This policy will apply from the date of effect and will be reviewed every 2 - 3 years or as required by best practice, legislation, or government policy changes.

Policy owner	Associate Director ICT & Business Services (Chief Information Security Officer)
This version endorsed by	PSC Management Board
Date endorsed	28/11/2023
Date effective	28/11/2023
Due for review	28/11/2026

Version no.	Endorsed date	Description of change
1.0	28/11/2023	Document created.

Appendix A: Data Breach Response Report

(Note: The content of any report to the NSW IPC must include those matters set out at s.59M of the PPIP Act; see also Appendix D below. When reporting to the IPC, copy the relevant details from this report into the IPC's approved form (see here), which must be completed unless it is not reasonably practicable.)

1. Contain and assess	
1.1	When did the Data Breach occur (if known)?
1.2	When, where, how and by whom was the Data Breach first discovered? (How long was the information exposed?)
1.3	When, how and by whom was the Data Breach first reported and to whom?
1.4	What was the primary cause of the Data Breach? • Malicious or criminal attack • System fault • Human error

1.5	Outline the nature of the Data Breach as first reported: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information/ Other: • Whether the breach is a cyber incident – details of the cyber incident • Cause of breach / how it occurred (provide a brief explanation) • Type of data affected: Financial information / Identity documents, credentials, and/or Government identifiers (e.g. Medicare, driver licence or passport numbers) / Tax File Numbers / Health information (including information about genetics or disability) / 'Sensitive information' (ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities) / Contact information (e.g. home address, phone number or email address) / Other types of personal information, third-party information • Type of individuals affected • Number of individuals affected (provide best estimate if figure if unknown) • Estimated cost of the breach to the agency
1.6	What steps were immediately taken to contain the Data Breach?
1.7	Who has been drafted into the Breach Response Team (SIRT)? (Include both internal and external stakeholders. Include the date the Breach Response Team was activated.)

1.8	Outline the results of the preliminary fact-finding, about: • Type of breach: Unauthorised access / Unauthorised disclosure / Loss / Alteration / Destruction of personal information • Cause of breach / how it occurred • The persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given • Type of cause: Cyber incident / Human error / Loss or theft of data or equipment / System fault / Other • If the breach was a cyber incident, provide details: Ransomware / Malware / Compromised credentials from phishing / Compromised credentials from brute force attack / Compromised credentials method unknown / Hacking / Other • A description of the data involved in the breach • Type of individuals affected • The nature of the harm that has occurred or may occur • Location of individuals affected • Number of individuals affected • Any other entity involved (e.g. a contracted service provider, other public sector agency or other type of third party) • Options to mitigate risk
1.9	What is the preliminary view as to the level of risk posed by the data breach? • High Risk (established) = likely to result in serious harm to affected individual/s • High Risk (suspected/possible, needs further investigation) • Medium Risk • Low Risk

1.10	Have any external parties been notified about the breach? E.g. our insurer; ID Support NSW; Cyber Security NSW; Australian Cyber Security Centre; police; other. (Include date and details.)
1.11 Other matters specified in the guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.	

2. Evaluate and Mitigate	
2.1	Who has now been drafted into the Breach Response Team (SIRT)? (Include internal and external stakeholders and when they were included.)
2.2	Remedial action: What steps have been taken to contain the Data Breach?
2.3	Remedial action: What steps have been / will be taken to minimise the effect on potentially affected individuals?
2.4	What steps have been / will be taken to prevent reoccurrence? (Consider here whether any similar breaches have occurred in the past.)
2.5	Concluding the assessment: What is the Breach Response Team's conclusion as to the level of risk posed by the data breach? (Include supporting reasons.) • High Risk = likely to result in serious harm to affected individual/s • Medium Risk • Low Risk

3. Notify and communicate	
3.1	Decision taken in relation to notification? (Include supporting reasons.) • Mandatory (all High Risk breaches) • Voluntary (optional for all other Medium Risk breaches) • No notification (Low Risk breaches)
3.2	Pre-notification steps concluded? (For example, establish telephone hotline, dedicated webpage. Include date completed and details.)
3.3	Report provided to the NSW Privacy Commissioner (IPC) under s.59M of the PPIP Act? (Use the approved form. Include date statement made, whether made on behalf of other agencies involved in the same data breach, how lodged. Attach a copy to this report.)
3.4	If TFNs were included: Statement provided to the Australian Privacy Commissioner (OAIC)? (Include date statement made, how lodged. Attach a copy to this report.)
3.5	What notification method/s have been followed for notifying affected individuals? • Direct to only individual/s at risk of serious harm • Direct to all individuals whose data was breached • Indirect via our website (mandatory if neither of the above is possible) • Indirect via other channels e.g. social media (an optional extra, in addition to one of the three methods above)
3.6	Notification made to affected individual/s? (Include date notification/s made, number of individuals notified, how many yet to be notified, how communicated.) Detail the contents of the notification, including what recommendations were made about the steps individuals could take to mitigate the effects of the breach; and whether they were advised of the complaints / internal review processes available to them under the PPIP Act. Attach a copy to this report.
3.7	Estimated cost of the breach to the agency?

4. Review and prevent	
4.1	What has been done to prevent a recurrence of this Data Breach?
4.2	Organisational response and mitigation plan. The following changes are recommended to our: • information security protocols • physical security controls • policies, plans or procedures • staff training / other
4.3	Recommended plan to review / audit to ensure the above corrective actions are implemented.

Appendix B: Factors to Consider in Assessing Serious Harm

The **assessment** about the **likelihood of serious harm** should have regard to:

1) the type of information involved: e.g. was it name and address, financial, health, criminal records, evidence of identity documents or other unique identifiers, biometrics, other types of 'sensitive information' such as information about a person's ethnicity, religion or sexuality? ('Sensitive information' is defined at s.19(1) of the PPIP Act.)
2) the volume of information involved: was it a combination of pieces of data about the individual which would not otherwise be known?
3) the number of individuals affected: e.g. is there a risk that due to the number of people impacted, there is a higher chance that someone in the cohort may experience serious harm as a result of the breach?
4) whether the information is protected by one or more security measures: e.g. what is the likelihood that any of the security measures could be overcome?
5) the risk profile of the information involved: e.g. could it be used for identity theft or other fraudulent purposes? to humiliate or blackmail the individual? to commit physical harm?
6) the type of individuals affected: e.g. are the individuals experiencing vulnerability (e.g. victims of family violence), or are the individuals involved worth targeting in some way (e.g. very wealthy people or public figures)?
7) how much time passed between becoming aware of the data breach and containing it?
8) the context: was this an isolated incident, a systemic problem, a deliberate attempt to steal data, or the result of an accident or other unintentional behaviour?
9) how likely is it, that the persons who may have obtained the information have an intention to cause harm to any of the individuals affected by the data breach?
10) the further effects: is there a risk of ongoing breaches or further exposure of the information?
11) the risk of cumulative harm: have there been breaches in other organisations that could result in a *cumulative* effect of more serious harm?

12) the extent to which the risk has been successfully prevented or lessened by any remedial action or containment efforts: e.g. was the data encrypted, was the portable storage device remotely wiped, were the hard copy files quickly recovered?

13) given all of the above, the type of harm likely to affect the individuals: e.g. identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of job opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalisation.

Appendix C: Contents of Mandatory Notification Statement

The mandatory notification statement to impacted individuals must set out:[6]

a) the date the breach occurred,
b) a description of the breach,
c) how the breach occurred,
d) the type of breach that occurred (i.e. unauthorised disclosure, unauthorised access, loss of information)
e) the personal information that was the subject of the breach,
f) the amount of time the personal information was disclosed for,
g) actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual,
h) recommendations about the steps the individual should take in response to the data breach (e.g. link to www.idcare.org if the breach suggests we need to assist individuals protect against identity theft),
i) information about making of privacy related complaints and internal reviews of certain conduct of public sector agencies,
j) the name and contact details of the public sector agency the subject of the breach,
k) if more than 1 public sector agency was the subject of the breach, the name of each other agency.

The mandatory notification statement to the Privacy Commissioner must use the approved form, and must set out:[7]

a) the information required to be provided to impacted individuals (as set out above),
b) a description of the personal information that was the subject of the breach,
c) whether the head of the agency is reporting on behalf of other agencies involved in the same breach,
d) if the head of the agency is reporting on behalf of other agencies involved in the same breach, the details of the other agencies,
e) whether the breach is a cyber incident,
f) if the breach is a cyber incident, details of the cyber incident,
g) the estimated cost of the breach to the agency,

[6] s.59O PPIP Act.
[7] S.59M(2) PPIP Act; see also the template form at https://www.ipc.nsw.gov.au/sites/default/files/2023-07/Form_Data_Breach_Notification_to_the_Privacy_Commissioner_July_2023.pdf.

h) the total number, or estimated total number, of individuals affected or likely to be affected by the breach, and notified of the breach,
i) whether the individuals notified have been advised of the complaints and internal review procedures under the PPIP Act.