information and privacy commission new south wales

NSW Mandatory Notification of Data Breach Scheme

A guide to managing data breaches in accordance with the Privacy and *Personal Information Protection Act 1998 (NSW)*

Updated July 2024

Contents

1 About this guide 3
1.1 Who should use this guide? 3
1.2 How to use this Guide 3
2 About the MNDB Scheme 3
2.1 Scope of application 4
2.2 Key terms 4
2.3 Interaction with the Commonwealth Notifiable Data Breach Scheme 6
2.4 Other reporting obligations 6
3 Data Breaches under the PPIP Act 7
3.1 What are the possible consequences of a data breach? 7
3.2 Interaction with the IPPs 7
3.3 MNDB Scheme overview 7
3.4 Key obligations under the MNDB Scheme 8
3.5 Privacy Commissioner's role under the MNDB Scheme 11
3.6 Breaches involving more than one agency 11
3.7 Breaches involving private sector service providers 12
4 Preparing for a data breach 12
4.1 Data Breach Policy 12
5 Responding to a data breach 13
5.1 Initial assessment and triage 13
5.2 Contain 14
5.3 Assess and mitigate 16
5.4 Notify 18
5.5 Review 22
6 Other resources 24

1 About this guide

Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) establishes the NSW Mandatory Notification of Data Breach (MNDB) scheme.

From 28 November 2023, every NSW public sector agency bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of eligible data breaches.

This Guide is intended to help NSW public sector agencies understand their roles and obligations under the MNDB Scheme. It establishes the Information and Privacy Commission's (**IPC**) expectations about what agencies should consider when dealing with a data breach and provides guidance to agencies about how data breaches should be assessed, managed and notified in accordance with legislative requirements.

1.1 Who should use this guide?

All NSW 'public sector agencies' (as defined in section 3 of the PPIP Act) should use this Guide to understand their obligations under the MNDB Scheme. This includes all NSW agencies and departments, statutory authorities, local councils, state-owned corporations, Ministers' offices and some universities.

From 28 November 2023, the definition of 'public sector agency' under the PPIP Act has been expanded to include NSW state-owned corporations (**SOCs**) that are not already captured by the Commonwealth *Privacy Act 1988* (**Privacy Act**).

1.2 How to use this Guide

This Guide is not prescriptive in nature and is not intended as a one-size-fits-all approach to managing data breaches. It is designed to be of general application to agencies of all sizes and in all sectors. The way an agency responds to a data breach will depend on the nature of the breach, the information involved, and the size and resources of the agency.

This Guide is not legal advice. It is published by the IPC to provide general information to help agencies understand their obligations under Part 6A of the PPIP Act. Agencies are encouraged to seek professional advice tailored to their own circumstances where required, including where seeking to rely on an exemption to the requirement to notify affected individuals.

This Guide is part of a suite of resources the IPC has developed to help agencies ensure they have the required systems, processes and capability in place, and should be used in conjunction with the Guide to Preparing a Data Breach Policy and other published resources.

The Privacy Commissioner has issued Guidelines which provides certainty to agencies on the intended meaning and limits of defined terms, guidance about what should be considered when assessing and managing a data breach, and how any exemptions may apply in relation to notification requirements.

2 About the MNDB Scheme

The MNDB Scheme requires public sector agencies to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm.

As part of the Scheme, agencies are required to publish a data breach policy, which outlines an agency's overall strategy for managing data breaches. Agencies must also maintain an internal register of eligible data breaches.

The MNDB Scheme has been established to ensure that both the Privacy Commissioner and affected individuals are notified when personal or health information is involved in a data breach, and there is a likelihood of serious harm to the affected individuals as a result. Notification allows people to take steps to reduce the risks of associated harms, for example by changing a password to online accounts, or monitoring for suspicious or fraudulent activity.

The MNDB Scheme serves another important purpose: to enhance transparency and accountability around privacy management within public sector agencies. Public sector agencies hold a wealth of information about individuals and have obligations to protect it. By holding agencies accountable and demonstrating that breaches of privacy are taken seriously and responded to appropriately, the MNDB Scheme builds trust in personal information handling across the NSW public sector.

2.1 Scope of application

The MNDB Scheme applies to 'eligible data breaches' involving 'personal information' or 'health information'. See section 3.5 below for a detailed discussion of those terms.

The MNDB Scheme applies to any public sector agency as defined in section 3 of the PPIP Act.

2.2 Key terms

The MNDB Scheme adopts several key terms, which are explained further in this section.

2.2.1 What is a data breach?

A data breach occurs when 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 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.

2.2.2 What is an eligible data breach?

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. [1]

The Privacy Commissioner has issued a Guideline to guide agencies through the considerations necessary for determining whether there has been an eligible data breach and whether the serious harm threshold has been met. Agencies must have regard to the Guideline when conducting an assessment under Part 6A of the PPIP Act.

2.2.3 Personal information and health information

The MNDB Scheme applies to breaches of 'personal information' as defined in section 4 of the PPIP Act - information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

The definition of personal information for the purposes of the MNDB Scheme includes 'health information', as defined in section 6 of the *Health Records and Information Privacy Act 2002* (**HRIP Act**).[2] This means that for the purposes of the MNDB Scheme (Part 6A of the PPIP Act only), 'personal information' includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

Expanding the definition of personal information to include health information for the purposes of the Scheme ensures that data breaches involving health information are treated in the same way as those involving other personal information, and that agencies take active steps to investigate, remediate and where appropriate, notify of such breaches.

2.2.4 What is serious harm?

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

[1] *Privacy and Personal Information Protection Act 1998* (PPIP Act), s59D

[2] PPIP Act, s59B

- 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.

The Privacy Commissioner has issued a Guideline which includes further information about the 'serious harm' threshold and the kinds of harm that may result from a data breach.

2.3 Interaction with the Commonwealth Notifiable Data Breach Scheme

The MNDB Scheme applies to NSW public sector agencies. In some cases, agencies will have notification obligations under both the MNDB Scheme and under the Commonwealth's Notifiable Data Breach (**NDB**) scheme, contained in Part IIIC of the Privacy Act.

For example, a data breach at a NSW public sector agency that involves Tax File Numbers and is likely to result in serious harm would be reportable to both the Office of the Australian Information Commissioner (**OAIC**) under the Commonwealth NDB scheme, and to the NSW Privacy Commissioner under the MNDB scheme.

The MNDB Scheme has been designed to be consistent with and adopt, as far as possible, key features of the Commonwealth NDB scheme. For example, the MNDB Scheme adopts the same thresholds for assessing and notifying data breaches so that agencies can meet both requirements with a single process.

2.4 Other reporting obligations

Agencies may be required, by other laws or administrative arrangements or by contract, to take specific steps in response to a data breach. These may include taking specific containment or remediation actions or notifying external stakeholders (in addition to the IPC or OAIC) when a data breach occurs. Depending on the circumstances of the data breach and the categories of data involved, agencies may need to engage with:

- Cyber Security NSW
- NSW Department of Customer Service
- NSW Police Force
- Australian Federal Police
- The Australian Taxation Office
- The Australian Digital Health Authority
- The Department of Health
- The Australian Cyber Security Centre
- Foreign regulatory agencies
- Professional associations, regulatory bodies or insurers
- Financial services providers
- Any third-party organisations or agencies whose data may be affected

3 Data Breaches under the PPIP Act

3.1 What are the possible consequences of a data breach?

Depending on the size or nature of a data breach, the consequences for individuals can be significant. They can give rise to a range of actual or potential harm to individuals. This harm can be physical, financial, emotional, or reputational and can include financial fraud, identity theft, damage to reputation and even threats of, or actual, violence. The characteristics and circumstances of the individuals affected may also impact the risk and type of harms associated with a breach, with greater consequences attached to those who are particularly vulnerable or at risk.

Data breaches can also have serious consequences for government agencies. A breach may create risk through the disclosure of commercially sensitive information, or otherwise impact an agency's reputation, finances, interests or operations. Ultimately, data breaches can lead to a loss of trust and confidence in an agency and the services it provides. For the NSW public sector, maintaining stakeholder trust is essential, particularly noting the nature of the relationship between the public sector and citizens: in some cases, failing to provide personal information to a public sector agency may mean a person is unable to access a critical government service or may otherwise breach their legal duties (for example, failing to provide their personal details when registering to vote).

Responding quickly when a data breach occurs can substantially reduce the impact of a breach on affected individuals, reduce the costs to agencies of dealing with a breach, and reduce the potential reputational damage that can result from a breach.

3.2 Interaction with the IPPs

Data breaches often involve, at least in part, a failure to effectively manage or comply with one or more of the 12 IPPs. By regulating the way agencies collect, store, use, disclose, and dispose of personal information, the IPPs ensure that privacy risks are minimised at each stage of the information handling process. Agency compliance with the IPPs, and with the PPIP Act generally, will help to reduce the risk of data breaches occurring. For example:

- The IPPs impose security obligations on agencies, requiring agencies to store personal information securely, and to protect it from unauthorised access, use, modification or disclosure.
- The IPPs limit the amount of information that may be exposed in a breach by:
    - Imposing data minimisation obligations on agencies, to limit the information collected about individuals.
    - Imposing retention and destruction obligations on agencies, requiring that information is kept no longer than necessary and is disposed of securely.

Later sections of this guide discuss other complementary measures which are part of agencies' overall approach to privacy, but which contribute to data breach prevention and response (such as staff training and awareness and operationalisation of their Privacy Management Plans).

Further information on the IPPs can be found in the IPC Fact sheet: IPPs for agencies.

3.3 MNDB Scheme overview

Agencies hold sensitive information about citizens, including personal, health and financial information. High-profile data breaches in Australia and internationally have demonstrated the potential for significant harm to individuals that can result from loss of, unauthorised access to, or unauthorised disclosure of, personal information. The MNDB Scheme improves public trust and helps mitigate the impact of data breaches when they occur by providing greater transparency, improving agencies' response to data breaches, and empowering affected individuals to take steps of their own to manage risks that might arise from a breach.

For Agencies, the MNDB Scheme imposes the following obligations:

- Where there are reasonable grounds to suspect that an eligible data breach may have occurred, agencies must:
  - Make all reasonable efforts to **contain** the breach,
  - **Assess** whether there has been unauthorised access to, or unauthorised disclosure of, personal information, or 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 within 30 days.
  - **Assess** whether there is a likelihood of serious harm to any affected individual within 30 days.
  - Make all reasonable attempts to **mitigate** the harm done by the suspected breach.
- Where a data breach has been assessed as an eligible data breach, agencies must:
  - **Notify** the Privacy Commissioner immediately, using the form approved by the Privacy Commissioner for this purpose and available on the IPC website.
  - **Notify** affected individuals as soon as practicable.
- Agencies must also maintain:
  - **A public data breach policy**, setting out how the agency will respond to a data breach.
  - **A public register of data breach notifications** issued by the agency.
  - **An internal register of eligible data breaches** at the agency.

The MNDB Scheme also gives the Privacy Commissioner a range of functions to support agencies in achieving best practice compliance, and to monitor and report on the performance of the Scheme. See section 3.5 below for further information on the powers and function of the Privacy Commissioner.

3.4 Key obligations under the MNDB Scheme

3.4.1 Publicly accessible Data Breach Policy

Agencies are required to prepare and publish a Data Breach Policy (**DBP**).[3] A DBP is a documented policy or plan setting out how an agency will respond to a data breach. It should establish the roles and responsibilities of agency staff in relation to managing a breach, and the steps the agency will follow when a breach occurs.

Agencies are required to ensure their DBP is publicly accessible. In practice, this means agencies should publish their DBP on their website. Agencies should also consider including a link to the policy on their intranet or other central repository and should ensure staff know how to access the policy.

See the Guide to preparing a data breach policy for guidance on how to prepare a DBP.

3.4.2 Contain and assess suspected breaches

The MNDB Scheme requires any officer or employee of a public sector agency with reasonable grounds to **suspect** that an eligible data breach has occurred to report this suspected breach to the head of the agency or their delegate.

The agency head must then carry out an assessment of whether there are reasonable grounds to believe that the suspected data breach is in fact an eligible data breach. This assessment must be completed within 30 days. Where an eligible data breach has occurred, the head of the agency must notify the Privacy Commissioner and affected individuals.[4]

[3] PPIP Act, s59ZD

[4] PPIP Act, s59E

On being made aware of a suspected breach, the head of the agency must immediately make all reasonable efforts to contain the breach. While the assessment is being conducted, the agency head must make all reasonable attempts to mitigate any harm done by the suspected breach. See Part 4 below for further information about containment and assessment measures.

Note, agency heads have powers to delegate their functions under the Scheme, including to employees in their agency.[5] Quick action is often key to successful data breach response. Agency heads should ensure appropriate delegations are in place so that the right people have the authority to make decisions quickly.

3.4.3 Notification obligations

Agencies must notify both the Privacy Commissioner and affected individuals of an eligible data breach.

Once the head of an agency determines that a data breach is an 'eligible data breach' for the purposes of the Scheme, they must:

- **Immediately** notify the Privacy Commissioner using the form approved by the Privacy Commissioner for this purpose which is available on the IPC website; and
- **As soon as practicable**, take reasonable steps to notify affected individuals (unless an exemption applies). If an agency is unable to directly notify any or all affected individuals, the agency must issue and publicise a public notification.

Notifications must be made using the approved form which is available on the IPC website. Agencies are welcome to seek advice from the IPC about a breach via a telephone call or email, but notification using the approved form is also required where there is an eligible data breach, in order to meet the notification requirements of the Scheme. A notification must include certain minimum details, such as information about the agency, the data breach, the impact on individuals and mitigation steps available to individuals.

An agency may be exempt from notification requirements to affected individuals where:

- A breach involved multiple agencies and another agency has undertaken to provide the notification.
- Notification would likely prejudice an investigation or court or tribunal proceedings.
- Mitigation action taken by the agency has prevented any likely serious harm resulting from the breach.
- Notification would be inconsistent with a secrecy provision in another Act.
- Notification would create a serious risk of harm to an individual's health or safety.
- Notification would compromise the agency's cyber security or lead to further breaches.

The above exemptions do not affect an agency's obligation to notify the Privacy Commissioner. Further information about notification requirements and exemptions is contained in Part 4 below.

3.4.4 Data breach incident register

Agencies must establish and maintain an internal register for eligible data breaches.[6] Each eligible data breach must be entered on the register, with the following information included for each entry where practicable:

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] *PPIP Act,* s 59ZJ.

[6] *PPIP Act,* s 59ZE.

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

Maintaining a data breach incident register is important for record-keeping and reporting purposes, as well as to comply with any request for information from the Privacy Commissioner.

3.4.5 Notification register

Agencies must maintain and publish (on their website) a public notification register for any public data breach notifications that the agency has issued.[7]

A "public data breach notification" is a notification made to the public at large rather than a direct notification to an identified individual. The MNDB Scheme provides for a public data breach notification to occur in two circumstances:

- a public notification **must** be made by an agency if it is unable, or it is not reasonably practicable, to notify any or all of the individuals affected by the breach directly,[8] or
- where an Agency head decides to make a public notification.[9] Agencies should note that the issuing of a public notification in these circumstances does not excuse the agency from the requirement to make direct notifications to affected individuals if it is reasonably practicable to do so.

The PPIP Act does not prescribe the information that must be included on the register. However, the purpose of the register is to ensure that citizens are able to access sufficient information about eligible data breaches to determine whether they may be affected by the breach and take action to protect their personal information. This means the agencies should provide information about:

- What happened
- What has been accessed
- What the agency is doing, and
- What an affected individual can do.

The IPC expects that the register should contain the following information:

a) the date the breach occurred
b) a description of the breach
c) the type of breach (unauthorised access, unauthorised disclosure or loss of information)
d) how the breach occurred
e) the type of personal information that was impacted by the breach
f) actions taken or planned to ensure that personal information is secure or to mitigate harm to individuals
g) recommended steps individuals should take in response to the breach
h) date the public notification was published
i) where to contact for assistance or information
j) a link to the full public notification.

Any public notification made by the agency must be published on the public notification register and remain available for at least 12 months after the date of publication.

---

[7] PPIP Act, s59P

[8] PPIP Act, s59N(2)

[9] PPIP Act, s59P(1)(b)

3.5 Privacy Commissioner's role under the MNDB Scheme

Under the MNDB Scheme, the Privacy Commissioner is empowered to work with agencies to facilitate legal compliance and privacy best practice, as well as to investigate and enforce the MNDB Scheme in the case of agency non-compliance.

The Privacy Commissioner has various powers under the Scheme, including to investigate, monitor, audit and report on the functions of an agency.[10] To facilitate this, the Privacy Commissioner has the power to access an agency's premises to observe its systems, policies and procedures.

The Privacy Commissioner is empowered to accept notifications from agencies of an eligible data breach. Under the Scheme is it an agency's responsibility to assess a breach and determine whether it is an eligible data breach. The Privacy Commissioner does not exercise a role to look behind the notification made by an agency on the basis that the agency is best placed to undertake the assessment with all available information concerning the data breach and its potential impacts. The Privacy Commissioner may exercise her regulatory functions to audit an agency's systems, policies and processes, including those established by the agency for the assessment of an eligible data breach.

As part of her functions under the Scheme the Privacy Commissioner monitors and provides regular reports on the operation of the scheme and the key lessons arising from the handling of data breaches. This will inform the development of future guidance to assist agencies to build and develop their practices, policies and systems. The Privacy Commissioner also issues regular statistical reports on data breach notifications made to the Commissioner.

3.6 Breaches involving more than one agency

The MNDB Scheme recognises that agencies often hold information jointly, and there may be situations in which the breach of personal information held by one agency must be managed across multiple agencies.

Under section 59C of the PPIP Act, an agency is taken to 'hold' personal information if:

a) the agency is in possession or control of the information, or
b) the information is contained in a state record in respect of which the agency is responsible under the *State Records Act 1998* (NSW).

Two agencies may 'hold' information jointly. For example, where one agency has physical custody of the record, while a second agency retains authority to determine what is done with the records.

In the event of a data breach affecting personal information that is jointly held between agencies, each agency is required to assess the breach and if the breach is determined to be an eligible breach, each agency must notify the Privacy Commissioner. However, only one of the affected agencies is required to notify affected individuals or make a public notification (if required).

The PPIP Act does not specify which agency is responsible for such notification. In general, the agency with the most direct relationship with the affected individuals will be best placed to notify and provide direct support as required.

[10] PPIP Act, Part 6A, Division 5

3.7 Breaches involving private sector service providers

The MNDB Scheme does not generally apply to private sector service providers providing services on behalf of government. This is because information held by a private sector service provider is usually 'held' by the service provider and not by a public sector agency.

However, as noted in section 3.6, an agency is taken to 'hold' personal information if the agency is in 'possession' or 'control' of the information. This means that information in the hands of a private sector service provider may still be 'held' by an agency if the agency retains a legal or practical power to deal with the personal information – whether or not the agency physically possesses or owns the medium on which the personal information is stored.

Some examples of when information in the hands of a private sector service provider may still be 'held' by the outsourcing agency include:

- Cloud-based IT services, also known as Software-as-a-Service (SAAS) or Infrastructure-as-a-Service (IAAS), where agency data is hosted on IT infrastructure owned and operated by the service provider.
- Physical archiving services, where agency hardcopy records are stored and maintained by the service provider.

Agencies holding personal information jointly with private sector service providers should incorporate the following in their procurement contracts:

- A requirement that the service provider promptly report data breaches to the agency, take mitigating actions and assist the agency in undertaking assessments.
- A statement of who should notify affected individuals and provide support in the event of the breach. As the organisation with the most direct relationship with the affected individuals the public sector agency will generally be best placed to notify and provide direct support as required.

4 Preparing for a data breach

4.1 Data Breach Policy

Agencies are required to prepare and publish a DBP. A DBP is a documented policy or plan setting out how an agency will respond to a data breach from start to finish. It should establish the roles and responsibilities of agency staff in relation to managing a breach, and the steps the agency will follow when a breach occurs.

Having a clear and well-defined DBP enables agencies to prepare for, evaluate, respond to and report on data breaches at the appropriate level and in a timely fashion, to mitigate potential harm to affected individuals and the agency itself, and to meet legal obligations.

Agencies are required to ensure their DBP is publicly accessible. In practice, this means agencies should publish their DBP on their website. Agencies should also consider including a link to the policy on their intranet or other central repository and should ensure staff know how to access the policy.

Agencies should refer to the Guide to preparing a data breach policy for in-depth guidance about how to prepare a DBP. Among other things, the guide covers:

- testing and exercising your DBP
- staff training and awareness
- processes for identifying and reporting data breaches
- roles and functions of a data breach response team, and
- data breach provisions in supplier contracts.

5 Responding to a data breach

Each data breach is unique and requires a tailored response. Response actions will depend on factors such as the type of data compromised, the cause of the breach, and the potential harms that could arise for affected individuals. It is important to understand the risks posed and respond to each breach accordingly.

While the details of each breach will be different, the process for responding to a data breach is always the same. Having a clearly defined process and well-defined roles and responsibilities for dealing with breaches enables agencies to respond quickly and effectively in an emergency.

The IPC recommends agencies follow six key steps:

1. **Initial report and triage:** Identifying, communicating and triaging breach reports.
2. **Contain:** Immediate action for containing the breach to prevent any further compromise of personal information.
3. **Assess and mitigate:** Assessing or evaluating the information involved in the breach and the risks associated with the breach to determine next steps and implementing any additional actions identified to mitigate risks.
4. **Notify:** Notifying the Privacy Commissioner and those affected by the breach.
5. **Review:** Reviewing and considering what actions can be taken to prevent future breaches.

5.1 Initial assessment and triage

To respond to a data breach, an agency must first know that it has occurred. Acting quickly when a breach is discovered or suspected is essential to reducing the impact for both the agency and affected individuals. Having a defined process for making, assessing and triaging breach reports will help agencies activate quickly when a breach is identified, and a report is made. This will also assist agencies to meet their obligation to undertake assessments in an expeditious way.

5.1.1 What are your obligations?

Any officer or employee of a public sector agency with reasonable grounds to suspect that an eligible data breach has occurred must immediately report the suspected breach to the head of the agency or their delegate.

5.1.2 Breach report protocols

To support staff to meet their reporting obligations, agencies should conduct awareness activities and have protocols in place for how suspected breaches are to be managed, assessed and reported. These should include:

- Staff training and awareness on how to identify a breach, what kinds of breaches may amount to an ‘eligible’’ data breach’, and how to make a report.
- Clear definition of roles and responsibilities regarding who can receive and action reports of suspected eligible data breaches, including when and how reports should be escalated.
- Guidance for agency heads, executive officers, privacy officers, or any other personnel who may be required to receive and action a report of a suspected breach.

We recommend that general agency staff be directed to report all suspected data breaches (whether or not they are likely to amount to an ‘eligible data breach’) to a central contact point. Reports can then be consistently assessed and documented by staff with relevant training and expertise.

Breach report protocols should be documented as part of an agency’s DBP.

5.1.3 Establish criteria for an escalated response

As part of the breach report process, agencies should establish a set of criteria for an escalated breach response (for example, the triggers for escalating reports to the Executive or convening a breach response team).

This could be based on the general criteria by which eligible breaches are to be assessed, such as:

- the type and sensitivity of information involved
- whether the information was protected by security measures
- the persons to whom the information was exposed, or
- the risk of harm to the individuals involved and the nature of any potential harm.

In addition, agencies could set specific escalation triggers, such as:

- the number of individuals affected
- any suspected external exposure of individuals' personal information
- any suspected unlawful activity
- any unauthorised use or disclosure (whether internal or between agencies) of certain categories of individuals' personal information – for example if users of a particular service are particularly vulnerable.

When in doubt, agencies should adopt a conservative approach and err on the side of escalation. Escalated incident response processes can be easily stood down if a breach turns out to be less serious than initially thought, but time lost when a serious incident is *not* escalated cannot be regained. In practice, agencies' training and escalation criteria could encourage staff to escalate when in doubt.

5.1.4 Convene an investigation / response team (if required)

Depending on the nature and severity of the breach, it may be necessary to convene a response team to manage the agency's response. An agency's DBP should establish clear criteria or triggers (discussed above) for escalation and should define the function or officer responsible for making decisions about convening a response team.

5.2 Contain

Upon becoming aware of a data breach, agencies must immediately make all reasonable efforts to contain the breach.

5.2.1 What are your obligations?

Under section 59E(2)(a) of the PPIP Act, once becoming aware that there are reasonable grounds to suspect there may have been an eligible data breach, the head of a public sector agency must immediately make all reasonable efforts to contain the breach.

'Containing' a data breach means limiting its extent, duration, or preventing it from intensifying. This could be done by:

- stopping an unauthorised practice,
- recovering or limiting the dissemination of records disclosed without authorisation,
- shutting down a compromised system or
- involve a combination of these actions.

Containment actions can be distinguished from mitigation actions, which involve managing or remediating harms arising because of the breach.

5.2.2 Possible containment measures

What efforts are reasonable to contain a breach will depend on the circumstances and severity of the breach, including:

- The type of data breach.
- Who has access to the personal information.
- The extent to which the breached personal information is still being shared, disclosed or lost without authorisation.
- The degree of harm that may result from continued exposure or dissemination of the records and the likelihood of such harm occurring, noting that agencies should mitigate even minor harms unless the cost, time and effort required to do so are excessively prohibitive.
- The availability and suitability of containment measures, considering their effectiveness, their impact on other individuals or agency operations, their practicality, and other relevant factors such as whether they would result in loss of evidence.

Some common types of containment actions include:

Context	Example containment actions
A letter has been sent to the wrong recipient.	• Contact the recipient and request the deletion of the personal information they have received. • If the personal information was highly sensitive, this could be evidenced by a statutory declaration or non-disclosure agreement.
A document is sent via a postal service and is lost in transit.	• Confirm (if possible) whether the document was properly addressed. • Contact the postal service to inquire as to the location of the document and whether it was confirmed as delivered. • Work with the postal service (if possible) to recover the document or confirm its destruction.
An email has been sent to the wrong recipient.	• Contact the recipient to: ○ request that they delete the email from their inbox and all trash items; and ○ seek confirmation that they have not forwarded or printed the document. • If the email or attachment was encrypted, it may be possible to remotely revoke access. • If the agency controls the recipient email inbox (for example, if the email was incorrectly sent to an internal recipient) it may be possible to recall or delete the email from the recipient inbox.
A physical asset (for example laptop, USB or phone) containing personal information has been lost or misplaced.	• Remotely wipe the device. • Work with police to locate and recover the device.
A system failure has resulted in a computer system exposing or distributing personal information in an unintended way.	• If practicable, shut down the system pending investigation and resolution of the issue. • Roll back to a previous software version that was not subject to the same issue.

A cyber-attack has led to the compromise of a system containing personal information.	• Isolate the system or compromised area of the system pending full investigation and response. • In extreme cases, a full system shutdown may be required
An employee has misused their valid credentials to access or disclose personal information outside the scope of their duties.	• Suspend the employee's system access pending full investigation.

During this preliminary stage, you should be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable you to address risks posed to affected individuals or your agency.

5.2.3 Special considerations when dealing with third-party breaches.

Data breaches involving third-party service providers are increasingly common, and present unique challenges for agencies. As noted in section 3.7 above, agencies should seek to include contractual terms in outsourcing arrangements that require service providers to report data breaches and cooperate with the agency in their breach response.

However, even with appropriate contractual powers in place, it can be difficult to take effective containment and mitigation actions or to conduct a timely and accurate assessment when the relevant information is split between the parties: the service provider having the knowledge about the system and the breach, while the agency possesses the contextual knowledge about the personal information needed to assess risk of serious harm.

When dealing with a third-party breach, agencies should:

- Engage their legal and procurement teams to review relevant contracts to understand parties' rights and obligations in detail.
- Work collaboratively with the third party to understand the nature and extent of the breach. Where the affected third party is a smaller service provider, this may include stepping in to assist them with containment or other steps.
- Where the affected third party is a large supplier with contracts across multiple public sector agencies, affected agencies should consider coordinating to jointly engage with the vendor on containment and remediation actions.

5.3 Assess and mitigate

5.3.1 What are an agency's obligations?

After a suspected data breach is reported to the head of an agency or their delegate, an assessment must be carried out within 30 days to determine whether there are reasonable grounds to believe that the suspected data breach is in fact an eligible data breach.[11]

Under section 59F of the PPIP Act, when assessing a data breach, the head of a public sector agency must make all reasonable attempts to mitigate the harm done by the suspected breach.

Taking steps to minimise or mitigate the harm caused by a data breach is a key element of any breach response.

[11] *PPIP Act,* s 59E(2)(b).

5.3.2 Assessing a data breach

There is no specific procedure by which an agency must conduct an assessment. In general, an assessment will involve the following:

1. **Information gathering:** collect all relevant information regarding the suspected breach. This may involve contacting relevant stakeholders, identifying what information was or may have been compromised, and investigating logs or other evidence from compromised systems that may be relevant to the assessment of the suspected breach.
2. **Analysis:** review the information collected during the previous phase to evaluate the scale, scope, and content of the suspected data breach and its potential impact on affected individuals.
3. **Decision:** come to a decision as to the eligibility of the suspected data breach based on the factors considered throughout the analysis.

More information on this process can be found in the Guideline on the assessment of data breaches to be issued by the Privacy Commissioner.

5.3.3 What can an agency do to mitigate the effects of a breach?

In practice, mitigation strategies will vary depending on the type and nature of the breach, and the potential harm to individuals the breach may cause. Notification, which enables affected individuals to take action to protect themselves, is the most common and most discussed mitigation measure. However, in many cases, additional mitigation steps are appropriate.

When a data breach affects certain individuals particularly severely, it may be appropriate to provide tailored support to meet their needs, which could include counselling, enhanced security, relocation assistance, or financial compensation.

When a data breach has an impact on a wider group of individuals, it may be more appropriate to focus on more scalable support options, such as helplines for advice about the breach, referral to specialist identity theft and cybersecurity counselling services such as ID Support, IDCare, or credit monitoring.

Other examples of mitigation measures include:

- Agencies may be able to implement additional security measures within their own systems and processes to limit the potential for misuse of compromised information. For example, by resetting passwords or adding additional requirements for proof of identity (POI) tests.
- Agencies may take steps to limit 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. Where information has been published, agencies may be able to contact internet search engines to ensure compromised personal information is not indexed. Agencies may also be able to engage with other websites on which compromised personal information may be displayed and ask them to remove the information.
- Agencies may engage 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, an agency may contact an identity issuer or financial institution to advise caution when relying on particular identity documents for particular cohorts, or to arrange for free replacement identity documents for affected individuals. (Note that any such engagement must be consistent with the IPPs).
- Where a data breach has led to direct financial harm, an agency may offer reimbursement. Agencies may also consider compensation for other types of harm.
- Where a data breach has exposed affected individuals to serious safety risks, an agency may support the installation of upgraded home security or cover relocation costs (if appropriate).

5.4 Notify

Transparency around how you handle people's information is central to good privacy practice. This extends to transparency when you suffer a breach and any personal information you hold is comprised.

Notifying affected individuals when a breach occurs allows them to take actions to protect themselves from harm and regain control of their information. Timely notification can be key to minimising the risks of serious harm resulting from a data breach.

5.4.1 What are your obligations?

When the head of an agency decides that 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, which are explained further in this section:

1. **Notify the Privacy Commissioner:** Once an agency determines an eligible data breach has occurred, the agency head must immediately notify the Privacy Commissioner about the breach in 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, an agency may not be required to notify affected individuals.
3. **Notify individuals:** Unless an exemption applies, agencies are required to notify affected individuals or their authorised representative as soon as reasonably practicable. Notification should be made directly to the individual concerned or their authorised representative. Where the agency is unable to notify directly or it is not reasonably practicable to do so, notification must be made publicly.
4. **Further information to be provided to the Privacy Commissioner:** Agencies may be required to provide additional information to the Privacy Commissioner, if they have been unable to provide complete information in their initial notification, if they have made a public notification, or if they are relying on an exemption.

5.4.2 Notification to Privacy Commissioner

If the head of a public sector agency decides that the data breach is an eligible breach, or that there are reasonable grounds to believe that the data breach is an eligible data breach, then the agency head must immediately notify the Privacy Commissioner.[12]

In some cases, it may be obvious that a breach will be an eligible breach even before the assessment is completed. If this is the case, agencies should consider notifying the Privacy Commissioner immediately rather than waiting until the assessment is finalised.

Notification to the Privacy Commissioner must be given in the approved form published by the Privacy Commissioner, and must include:

- The information that will need to be provided to individuals if no exemption applies (see below).
- The following additional information:
    - A description of the personal information that was subject to the breach.
    - Whether the head of the agency is reporting on behalf of other agencies involved in the breach.
    - Whether the breach is a cyber incident and details of the cyber incident (if applicable).
    - The estimated cost of the breach to the agency.

[12] PPIP Act, s59M

- The total number (or estimate) of individuals:
  - affected or likely affected by the breach, and
  - notified of the breach.
- Whether the individuals have been notified of the complaints and review procedures.

Agencies may omit information from their notification to the Privacy Commissioner if it is not reasonably practicable to provide it. For example, notification may occur before final completion of an agency's incident response and investigation, so it may not yet be confirmed how the breach occurred and may not be possible to provide a complete list of actions taken or planned to secure the information or control or mitigate harm to individuals. Similarly, notification to the Privacy Commissioner will usually occur before notification to individuals, so it may not be possible to advise the total number of individuals notified.

Agencies must provide a follow-up notification to the Privacy Commissioner of any information that was not included in their original notification.[13] Follow-up notifications must also be provided in the approved form.

5.4.3 Does an exemption apply?

After notifying the Privacy Commissioner, agencies must notify individuals unless an exemption applies. The exemptions are:

- Where an eligible data breach affects multiple public sector agencies, and another agency has undertaken to notify individuals. Both agencies must still conduct their own assessment, containment and mitigation, and notify the Privacy Commissioner.[14]
- Where notification of the eligible data breach would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or a tribunal.[15]
- Where the agency has taken mitigation action that successfully prevents serious harm from occurring, so that a reasonable person would conclude that the breach is no longer likely to result in serious harm to an individual.[16]
- Where notification would be inconsistent with a secrecy provision in another Act.[17]
- Where notification would create a serious risk of harm to an individual's health or safety.[18]
- Where notification would worsen the agency's cyber security or lead to further breaches.[19]

Agencies relying on exemptions relating to health or safety or cyber security must provide a written notice to the Privacy Commissioner advising of their reliance on the exemption and provide other specified information. Agencies should keep appropriate records of any assessment and decision-making process leading to reliance on an exemption.

Further information about the application of the exemptions can be found in the Privacy Commissioner's Guidelines.

---

[13] PPIP Act, s59Q

[14] PPIP Act, s 59S.

[15] *PPIP Act,* s 59T.

[16] *PPIP Act,* s 59U.

[17] *PPIP Act,* s 59V.

[18] *PPIP Act,* s 59W.

[19] *PPIP Act,* s 59X.

5.4.4 Notification to individuals

If there is an eligible data breach and none of the exemptions apply, agencies must notify relevant individuals of the eligible data breach.

5.4.4.1 Who must be notified?

Agencies may elect to notify either:

1. Each individual to whom the compromised information relates, regardless of their risk of harm; or
2. Only affected individuals, meaning those individuals who are likely to suffer serious harm as a result of the compromise of personal information that relates to them.[20]

If an agency is unable, or it is not reasonably practicable, to notify all relevant individuals, an agency must issue a public notification instead (see below). For example, notification to all relevant individuals may be impossible or not reasonably practicable if the agency does not hold (and cannot practicably obtain) current, direct contact details for some or all of the affected individuals.

5.4.4.2 When should agencies notify?

Notification to individuals must be made 'as soon as reasonably practicable' after determining that a breach is an eligible data breach.

Timely notification is important to help affected individuals affected by a breach take personal steps to limit or mitigate the risks of misuse or further exposure. Agencies should avoid undue delay and should work to make affected individuals aware of the breach as soon as possible.

Agencies should carefully balance speedy notification to individuals with ensuring that citizens are provided with reliable and accurate information about the breach. Most importantly, notifications should provide recipients with an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves. If an agency is not yet able to provide meaningful detail in a data breach notification, it may be too early to provide it.

Similarly, a notification that gets things wrong can cause more harm than good. A notification that provides inaccurate advice about what information has been breached or provides incorrect advice about who may be at risk, can cause unnecessary anxiety and stress in those not seriously affected and may fail to achieve the central objective of enabling those who are affected from taking protective action.

For complex breaches or where significant numbers of individuals are affected, the agency may need to consider applying a triage system to notification. This might involve making notification in tranches based on the level of risk posed to the individual or the sensitivity of the information involved in the data breach.

5.4.4.3 What should be included in the notification?

For most people, receiving a notification that their personal information has been breached can be very stressful. In some cases, it can have a significant impact on an individual's emotional and psychological wellbeing, particularly where they are at risk or especially vulnerable.

The way you tell people that their information has been breached is important. Notifications should avoid minimising the severity of a breach, but also seek to avoid causing undue alarm. Notifications should provide recipients with an accurate sense of what happened, what risks may arise, and what they can do to protect themselves. Notifications should be made in plain English, using clear and easily understood language.

[20] PPIP Act, s59N

A notification should generally be made in writing. Agencies should consider how notifications will be sent to the affected individuals: by registered post, regular post, email, push notification via an agency app, etc. The method chosen may depend on the type of contact information held by the agency.

In some instances, such as where the individual may be at imminent risk of physical violence as a result of a data breach, a notification by phone may be appropriate. This should always be followed by a written notification.

Section 59O of the PPIP Act sets out specific information that must, if reasonably practicable, be included in a notification:

a) the date the breach occurred
b) a description of the breach
c) how the breach occurred
d) the type of breach that occurred
e) the personal information included in the breach
f) the amount of time the personal information was disclosed for
g) actions that have been taken or are planned to secure the information, or to control and mitigate the harm done
h) recommendations about the steps an individual should take in response to the breach
i) information about complaints and reviews of agency conduct
j) the name of the agencies that were subject to the breach
k) contact details for the agency subject to the breach or the nominated individual to contact about the breach.

5.4.4.4 Public notification

If it is not reasonably practicable to notify any or all of the individuals affected by the breach directly, an agency must issue a public notification instead. Direct notification may be impracticable for a range of reasons, such as where a breach involves older records, and the agency does not hold current, direct contact details for some or all of the affected individuals.

Agency heads may also decide to make a public notification concurrently with direct notifications to affected individuals. The issuing of a public notification in these circumstances does not excuse the agency from the requirement to make direct notifications if it is reasonably practicable to do so.

A public notification must include all the same information that would be included in a direct notification, but should exclude:

- personal information about an individual. For example, an agency may exclude information about specific individuals involved in the breach or breach response.
- information that would prejudice the agency's functions. For example, an agency may omit certain details about a breach if they would expose a confidential investigation or publicise a vulnerability that still exists and can be further exploited.

Agencies making a public notification must:

- Keep a public notification register on their website (see section 3.4.5 for further details).
- Publish the notification on the public notification register for at least 12 months.
- Advise the Privacy Commissioner of how to access the notification on the public register (for example, by emailing the link to the notification website).

In addition to publishing the notification on their website, agencies must take reasonable steps to publicise the contents of the statement, to increase the likelihood that it will come to the attention of those individuals at risk of serious harm. This could be through any appropriate channels available to the agency, such as a media release, a notice on the main agency website, a recorded message on the agency's customer service line, direct communications with stakeholders or affected individuals who are contactable, or by paid advertising.

Agencies are strongly encouraged to consider utilising more than one channel to ensure that the public notice is effectively communicated to individuals.

5.4.4.5 Further information to Privacy Commissioner

Notification of an eligible data breach to the Privacy Commissioner will not usually be a once-off. Agencies should seek to keep the Privacy Commissioner updated as the breach response progresses, and new information comes to light. The MNDB Scheme includes several further requirements on agencies to update the Privacy Commissioner on their breach response and approach to notification:

- If an agency omits information from its immediate notification to the Privacy Commissioner, it is required to provide an updated notification once that information becomes available. This is usually once their incident response process has been completed and individuals have been notified of the breach (or an exemption has been determined to apply). See section 5.4.2.
- If an agency relies on either of the exemptions relating to health or safety or cyber security, they must additionally provide a written notice to the Privacy Commissioner advising of their reliance on the exemption, whether the exemption is permanent or temporary, and if temporary, the expected time the exemption is to be relied on. See section 5.4.3.
- If an agency publishes a public notification, it must advise the Privacy Commissioner of how to access the notification on the public register (for example, by emailing the link to the notification website). See section 5.4.4.4.

5.4.4.6 Collection, use and disclosure of personal information for notification

Section 59R of the PPIP Act provides that an agency may collect, use or disclose personal information for the purpose of confirming:

a) the accuracy of the name and contact details of an affected person or a person whose personal information has been compromised, or
b) whether that person is deceased.

The provision provides agencies with a limited exemption to the obligation to comply with an IPP, a Health Privacy Principle, a privacy code of practice or a health privacy code of practice. The exemption only permits collection and disclosure of personal information between agencies, and only so far as reasonably necessary for the above purposes. Additionally, the exemption is limited to the following types of personal information:

a) the name of an individual
b) the contact details of the individual
c) the date of birth of the individual
d) an identifier for the individual (for example, NSW driver license number)
e) if the individual is deceased—the date of death of the individual.

5.5 Review

Dealing with a data breach extends beyond immediate assessment and notification requirements. Understanding what went wrong, how issues were addressed and whether changes to systems, processes and procedures following a breach will mitigate future risks, is key to ensuring agencies continue to proactively manage data breaches in line with regulator and community expectations.

Agencies should consider a data breach incident as an opportunity to review and strengthen information security and data handling practices. A post incident review will often highlight processes that are vulnerable to human error or weaknesses in existing systems and security controls that should be addressed to reduce the likelihood of future breaches.

5.5.1 Documenting issues and remedies

Following a data breach, agencies should take time to investigate what went wrong and to update relevant policies and procedures to remedy any issues to prevent future breaches.

A post incident review should cover:

- The effectiveness of the agency's Data Breach Policy and incident response process itself.
- A root cause analysis of the data breach.
- If required, more focused reviews of particular systems, policies and procedures involved in the breach. For example,
    - If the breach exposed a large number of old and unnecessary records, a review of the agency's data retention and deletion processes.
    - If the breach involved human error in a manual process, a review of how the process might be made safer.
    - If the data breach involved a security flaw in a particular system or collection of systems, a security review and root cause analysis.
    - If the data breach involved a supplier, a review of that supplier's contractual arrangements and security posture.

Agencies should document agreed remediation actions arising from the post incident review in their Privacy Management Plan.

5.5.2 Review and update data breach policy

It is common for agencies to identify opportunities for improvement in the DBP and breach response process itself after each data breach response. Processes, thresholds, escalation and reporting pathways that sounded reasonable when the DBP was drafted may be ineffective in practice. To take advantage of these learnings, an agency's DBP should be reviewed after every breach response and updated to address any opportunities for improvement that may have been identified.

5.5.3 Preventing future breaches

This section lists possible preventative measures to address specific types of breaches, which may assist agencies to identify potential pathways to improvement after a data breach. It is not intended to be prescriptive or exhaustive.

5.5.3.1 Breaches involving the sharing of information with unintended recipients

If the breach was caused by the accidental sharing of an email or other type of communication to unintended recipients, preventative measures could include:

- Ensuring staff are aware of, and receive training on, the NSW Government Information Classification, Labelling and Handling Guidelines.[21]
- Establishing alternative processes and systems so that highly sensitive documents or information are not shared by email.
- Encouraging staff to send links to files rather than full file attachments where possible.
- Using passwords/encryption to protect documents containing sensitive information or large amounts of personal information.
- Training employees to consider whether an entire document or spreadsheet needs to be sent or if there is a way of extracting only the relevant information intended for the recipient.

[21] https://arp.nsw.gov.au/dcs-2020-07-nsw-government-information-classification-labelling-and-handling-guidelines/.

5.5.3.2 Breaches involving the theft or loss of devices

If the breach was caused by the theft or loss of devices, preventative measures could include:

- Establishing a policy for the types of information that can be stored on a portable device.
- Imposing additional security measures for portable devices such as encryption, password locks, multi factor authentication, remote wiping and physical security.
- Protecting sensitive documents and information using physical security measures such as locks or filing cabinets.
- Training staff to ensure documents, computers or other electronic devices are not visible in homes or in parked cars.
- Establishing a protocol for deleting personal information and other data when it is no longer needed in accordance with the retention requirements under the *State Records Act*.

5.5.3.3 Breaches involving malicious online attacks

If the breach was caused by malicious online attacks, preventative measures could include:

- Investing in your agency's security capability and maturity.
- Applying mitigation strategies such as the Australian Cyber Security Centre's Essential Eight.
- Applying a cybersecurity risk management framework such as the US Government's National Institute of Standards and Technology (NIST) Cyber Security Framework.
- Requiring multi-factor authentication and the use of strong passwords for all employee accounts.
- Investing in regular employee training on IT security.
- Undertaking a regular phishing simulation program to test staff awareness of, and capacity to identify, suspicious emails.
- Restricting employees' ability to install software onto work computers.

5.5.3.4 Breaches involving unauthorised access and/or disclosure by employees

If the breach was caused by unauthorised access or disclosure by employees, preventative measures could include:

- Instituting role-based access to files (e.g., locking files down and only providing access to those employees with a need to know).
- Logging and monitoring employee access to files, flagging and investigating unusual or suspicious activity, and taking disciplinary action where appropriate.
- Clearly establishing in your agency's code of conduct that access to personal information is on a need-to-know basis, with clear consequences for violations of the code.
- Training staff on the handling and management or personal information, including organisational practices around monitoring and auditing of file access.

6 Other resources

Links to complementary resources are located below.

- Mandatory Notification of Data Breach Scheme
- Guide to preparing a data breach policy
- Privacy Resources for Agencies (nsw.gov.au)
- Cyber Security NSW
- NSW Cyber Security Incident Emergency Sub Plan
- Data breach preparation and response - Home (oaic.gov.au)

NOTE: The information in this Guideline is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.

Document information

Identifier/Title:	Mandatory Notification of Data Breach Scheme
Business Unit:	IPC
Author:	Legal Counsel and Regulatory Advice
Approver:	Privacy Commissioner
Date of Effect:	15 June 2023
Next Review Date:	15 June 2025
EDRMS File Reference:	D23/019891/DJ
Key Words:	Data breach, notifications, compliance obligations, data breach preparation and response