

# ADC Data Breach Policy

## Table of contents

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>Introduction .....</b>                                        | <b>3</b>  |
| <b>What is a data breach? .....</b>                              | <b>3</b>  |
| <b>What is an eligible data breach? .....</b>                    | <b>4</b>  |
| <b>Roles and responsibilities .....</b>                          | <b>5</b>  |
| <b>Processes and systems to prepare for a data breach .....</b>  | <b>6</b>  |
| <b>Responding to a data breach .....</b>                         | <b>7</b>  |
| <b>Step 1: Contain, assess and report a data breach .....</b>    | <b>7</b>  |
| <b>1.1 Containing the breach .....</b>                           | <b>7</b>  |
| <b>1.2 Initial assessment and reporting .....</b>                | <b>8</b>  |
| <b>Step 2: Notification .....</b>                                | <b>11</b> |
| <b>2.1 Where the breach is an eligible data breach .....</b>     | <b>11</b> |
| <b>2.2 Where the breach is not an eligible data breach .....</b> | <b>15</b> |
| <b>Step 3: Review and learn .....</b>                            | <b>15</b> |
| <b>Related documents .....</b>                                   | <b>16</b> |
| <b>Relevant legislation .....</b>                                | <b>16</b> |
| <b>Document information .....</b>                                | <b>16</b> |

## Introduction

A timely and effective approach to responding to data breaches can reduce the impact of a breach on individuals and the Ageing and Disability Commission (ADC) and can help to prevent future breaches.

The ADC is subject to the Mandatory Notification of Data Breach (MNDB) Scheme, which is established under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act). Under the MNDB Scheme, the ADC must notify the Privacy Commissioner<sup>1</sup> and affected individuals of ‘eligible data breaches.’ The MNDB Scheme also requires us to publish a Data Breach Policy and maintain an internal register and public register of eligible data breaches.

This Policy provides guidance to ADC staff and contractors on how to respond to a data breach (or suspected data breach) of ADC-held personal information, in accordance with the requirements of the PPIP Act.

This Policy outlines:

- how to identify a data breach, including an eligible data breach
- the roles and responsibilities for reporting, managing and reviewing data breaches
- the steps involved in dealing with a data breach and preventing future data breaches.

This Policy applies to all staff and contractors of the ADC, including temporary and casual staff, and private contractors. This Policy also applies to third party providers who hold personal information on behalf of the ADC.

The Director Operations is the Delegate in relation to the ADC’s execution of the MNDB Scheme.

## What is a data breach?

A **data breach** occurs when personal information, including health information, held by the ADC is lost or subject to unauthorised access or unauthorised disclosure.

‘Personal information’ is defined in section 4 of the PPIP Act to mean information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including:

- a record which contains personal details about a person including, but not limited to:
  - name
  - address
  - phone number
  - date of birth
  - ethnic or racial origin
  - religious or philosophical beliefs
  - photographs, images, video or audio footage.

---

<sup>1</sup> All references in this policy to the Privacy Commissioner refer to the ‘Privacy Commissioner’; all references to the Ageing and Disability Commissioner refer to ‘the Commissioner’.

‘Health information’ is defined in section 6 of the *Health Records and Information Privacy Act 2002* (HRIP Act) to include information or an opinion about an individual’s physical or mental health, disability, and information connected to the provision of a health service.

For the purposes of this Policy, a reference to ‘personal information’ includes a reference to ‘health information’.

Personal information is ‘held’ by the ADC if:

- the ADC is in possession or control of the information; or
- the information is contained in a State record in respect of which the ADC is responsible under the *State Records Act 1998*.

A data breach can be accidental or intentional and may arise as a consequence of a cyber-attack, inadvertent disclosure, over-provisioning of access to sensitive systems, or as a result of loss or theft of a physical device.

Types of data breaches include:

- loss or theft of a device containing ADC information, for example a loss of a USB stick or a case file
- an ADC database or information repository being compromised or accessed without authorisation, for example the sharing of user login details with a third party, hacking, or malware infection
- an ADC employee or contractor mistakenly providing personal information to an unauthorised person or entity, for example by sending an email containing personal information to the wrong recipient.

## What is an eligible data breach?

The MNDB Scheme applies where an **eligible data breach** has occurred. An eligible data breach occurs when there is a data breach and 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.

A ‘reasonable person’ is a hypothetical individual who is properly informed with sound judgement.

**Serious harm** occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect on an individual. Harm to an individual includes physical, economic, financial, social, emotional, psychological or reputational harm.

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

The NSW Privacy Commissioner’s statutory guidelines will be considered by the ADC in its assessment of all data breaches affecting the ADC<sup>2</sup>.

---

<sup>2</sup> See <https://www.ipc.nsw.gov.au/privacy/MNDB-scheme>.

The harm(s) that can arise because of a data breach will vary depending on the circumstances. For example:

- the type and level of sensitivity of personal information accessed, disclosed or lost
- the circumstances in which the data breach occurred
- the amount of time the personal information was exposed or accessible
- the circumstances of the individual affected, and their vulnerability or susceptibility to harm
- the persons who were provided unauthorised access to the personal information, and the likelihood of them misusing that information
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm to an individual may include:

| Type of harm                              | Example                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Physical, psychological or emotional harm | An individual is subjected to threats to their physical safety or harassment after another person gains unauthorised access to their personal information.<br><br>Note: the harm to some individuals may be exacerbated due to their personal circumstances or profession (for example, individuals affected by family or domestic violence, police officers, judicial officers). |
| Financial or material harm                | An individual is exposed to identity theft or fraud after their identity documents were disclosed without authorisation.                                                                                                                                                                                                                                                          |
| Reputational harm or discrimination       | An individual is exposed to discrimination or their reputation is damaged due to unauthorised disclosure of information regarding their medical history or criminal history.                                                                                                                                                                                                      |

## Roles and responsibilities

The following ADC staff have identified roles under this Policy:

| Role                 | Responsibilities include                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Director, Operations | <ul style="list-style-type: none"> <li>• Receive reports of suspected eligible data breaches and coordinate the response.</li> <li>• Review and approve recommendations made by business unit managers.</li> <li>• Consult with reporting business unit before finalising an assessment or proposed actions or recommendations.</li> <li>• Coordinate notification to the IPC, affected individuals, and external bodies.</li> <li>• Ensure maintenance of the internal data breach register.</li> <li>• Provide the ADC Executive and Audit and Risk Subcommittee with an update on any data breaches at least on a quarterly basis.</li> </ul> |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | <ul style="list-style-type: none"> <li>Review and update the Data Breach Policy as required.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ADC business unit managers             | <ul style="list-style-type: none"> <li>Report a suspected eligible data breach to the Director in accordance with this Policy.</li> <li>Undertake assessment of suspected data breaches in their business unit, including identification of cause and recommendations for preventative/remedial action.</li> <li>Assist in containment, mitigation of harm, and implementation of preventative/remedial action.</li> <li>Ensure that any data breaches or suspected data breaches and subsequent actions are recorded in the ADC Data Breach Register.</li> </ul> |
| DCJ IDS Business Partner               | <ul style="list-style-type: none"> <li>Establish the cause and impact of a breach involving DCJ IT systems.</li> <li>Assist in containment, mitigation of harm, and implementation of preventative/remedial action.</li> <li>Provide information to assist in the assessment of data breaches.</li> <li>Provide advice on review of security and monitoring controls related to breaches, and preventative or remedial action.</li> </ul>                                                                                                                         |
| Commissioner                           | <ul style="list-style-type: none"> <li>Maintain a high-level overview of eligible data breaches and provide advice as needed on responses.</li> <li>Review matters referred by the Director for decision.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Manager, Communications and Engagement | <ul style="list-style-type: none"> <li>Maintain the public notification register and publish public notifications on the ADC's website.</li> <li>Respond to enquiries from media and external stakeholders.</li> </ul>                                                                                                                                                                                                                                                                                                                                            |
| ADC staff and contractors              | <ul style="list-style-type: none"> <li>Immediately report a data breach or suspected data breach to their line manager in accordance with this Policy.</li> <li>In consultation with their line manager, take reasonable steps to contain a data breach and mitigate any potential harm that may result from a data breach.</li> <li>Take steps to prevent recurrence of a data breach.</li> <li>Participate in training on responding to data breaches.</li> </ul>                                                                                               |

## Processes and systems to prepare for a data breach

The ADC's IT network and infrastructure is managed by the Department of Communities and Justice (DCJ), which has implemented a number of cyber security measures to mitigate the risk of data breaches. This includes:

- automated password updates so ADC staff regularly change their computer login password
- email alerts sent to staff regarding cyber vulnerabilities and fixes
- cyber security training to assist staff to identify possible causes of data breaches and how to detect and report suspicious online activity.

DCJ and the ADC have also implemented the following practices to prepare for and to assist in mitigating data breaches:

- data loss prevention practices
- persistent dark web monitoring
- information security hints and tips
- fact sheets on various privacy topics, including checking email attachments.

Where it is necessary for personal information to be transferred to a third party in connection with the provision of a service to us, we ensure that our contracts or memoranda of understanding or agreements with these third-party service providers include provisions:

- in relation to the management and notification of data breaches
- that impose privacy obligations to ensure that the parties comply with the PPIP Act and HRIP Act.

The ADC will ensure all third-party service providers who receive ADC-held personal information in connection with the provision of a service to us, are aware of the MNDB Scheme and the obligations under this Policy to report any data breaches to the ADC.

## Responding to a data breach

How we respond to a data breach in the initial 24–48 hours is critical to its effective management.

The ADC's procedure for responding to a data breach comprises the steps set out below. The flowchart in **Appendix A** outlines the sequence of the steps that need to be taken.

### Step 1: Contain, assess and report a data breach

#### 1.1 Containing the breach

An **immediate priority** is to contain the breach. All necessary and possible steps must be taken to prevent any further loss or compromise of personal information and to minimise any potential harm to affected individuals.

Once you have attempted to contain the breach, you must immediately notify your line manager.

Each data breach is unique and how you contain it will be determined on a case-by-case basis. To identify the appropriate strategy to contain the data breach, consider:

- How did the breach occur?

- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

Examples of how you may need to contain a data breach may include, but are not limited to:

- retrieving the information and/or preventing any further disclosure, misuse of loss – for example, recalling emails sent to an incorrect address or requesting the email be deleted or the information destroyed and returned to the ADC
- suspending the activity that led to the breach
- shutting down the system that caused the breach and addressing security weaknesses
- revoking or changing passwords or access codes
- contacting affected parties to enable them to take proactive steps to limit the impact of the data breach
- if the ADC becomes aware that the personal information has been published on a public site or platform, seeking the immediate removal of the information from the site or platform.

If a third party receives the personal information of another person in error and the correspondence cannot be recalled, the third party must be contacted by the fastest means possible (telephone or email) to inform them of the breach of privacy, and to instruct them to return or destroy the information, or to delete any electronic records without first reading, making copies, or forwarding to any other party. If the third party is contacted by telephone, this must be followed by written correspondence to the third party, asking them to confirm that they have not retained any copies of the information in their possession.

When implementing a containment strategy, it is important not to destroy any evidence that may be valuable in identifying the cause of the breach.

## 1.2 Initial assessment and reporting

The manager of the business unit where the breach originated must make an initial assessment as to whether there are reasonable grounds to suspect that the breach is an eligible data breach.

As noted in ‘**What is an eligible data breach?**’ above, an eligible data breach is one that meets the following two conditions:

- a) there is unauthorised access to, or unauthorised disclosure of, personal information, or personal information held by a public sector agency is lost; and
- b) a reasonable person would conclude that the unauthorised access or disclosure would be likely to result in serious harm to an individual to whom the information relates (‘affected individual’).

‘Serious harm’ is assessed by considering the severity of the potential or actual impact arising from the data breach on an affected individual. Relevant considerations include the likelihood

of a particular harm occurring, as well as the anticipated consequences for affected individuals whose personal information is involved in the data breach if the harm materialises.

The ADC's Privacy Risk Matrix (**Appendix C**) should be used to assess the level of risk, consequences and serious harm arising from a data breach.

When making an initial assessment of whether a data breach would be likely to result in serious harm to affected individuals, you should consider:

- The type(s) and sensitivity of the personal information involved in the data breach – see **Appendix D** for examples of the types of personal information that is likely to be higher in risk.
- Whether the personal information relates to vulnerable cohorts that increases the risk of serious harm. For example, information about an adult with disability, older person, or child/young person.
- Whether the personal information is protected by any security measures.
- Whether the data breach was caused by or related to a cyber incident.
- Any persons who have obtained, or who could obtain the personal information and whether there is any likelihood of those persons causing harm or circumventing security measures.
- The nature of the harm that has occurred or may occur.
- Whether the data breach is the result of a malicious attack on ADC infrastructure or assets.
- Whether the breach or suspected breach impacts other government or non-government agencies.
- Whether the breach or suspected data breach could attract media attention.

When using the above points to assess the risk of 'serious harm', the ADC should consider the broad range of risks that may flow from a data breach including, but not limited to:

- identity theft
- threats to physical safety, including personal or domestic violence
- humiliation, damage to reputation or relationships
- significant media/social media attention
- significant financial loss
- loss of business or employment opportunities
- workplace or social bullying or marginalisation.

If there is any doubt as to whether an eligible data breach has occurred, or may have occurred, the matter should be reported to the Director for confirmation.

**If it is assessed as a DATA BREACH (no likelihood of serious harm to any affected individual):**

Within seven (7) working days, the business unit must:

- document the reasons for the decision using the Reporting Form at **Appendix B**
- identify any steps taken to address the incident (for example, recalled emails, training)
- consider changes to processes and/or procedures to mitigate any recurrence as necessary
- email the reporting form and any related evidence to the Director

- complete the Data Breach Register in TRIM.

If further information comes to light after conducting an initial assessment that changes the original classification of the data breach to an eligible data breach, the business unit must conduct a further assessment.

#### **If it is identified as a suspected ELIGIBLE DATA BREACH:**

Where a suspected eligible data breach has been identified, the manager of the relevant business unit will:

- immediately email the Director to advise of the suspected data breach
- if the breach is a cyber incident, contact DCJ IT on [security.incident@dcj.nsw.gov.au](mailto:security.incident@dcj.nsw.gov.au) (during business hours) or 1300 325 29237 (after hours)
- within seven (7) working days, complete an assessment of whether the reported breach is an eligible data breach under the MNDB Scheme, using the Reporting Form (**Appendix B**), Privacy Risk Matrix (**Appendix C**) and Personal Information Risk Matrix (**Appendix D**), and send the reporting form to the Director
- identify any steps taken to address the incident (for example, recalled emails, training)
- consider changes to processes and/or procedures to mitigate any recurrence as necessary
- complete the Data Breach Register in TRIM. The register is to be updated with further information as the matter progresses.

The assessment will have regard to guidelines issued by the Privacy Commissioner about the process for carrying out an assessment.

Section 59H of the PPIP Act sets out a non-exhaustive list of factors that may be considered in carrying out the assessment of whether the data breach is (or there are reasonable grounds to believe the data breach is) an eligible data breach. Factors to consider include:

| Factor                                                | Considerations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What personal information was involved in the breach? | <p>Some types of information are more likely to cause harm if it is compromised. For example, security-protected information, or sensitive personal or health information are more significant than disclosure of personal information such as names or email addresses only.</p> <p>A combination of personal information will typically create a greater potential for harm than a single piece of information. For example, date of birth and bank account details, if combined, could be used for identity theft).</p> |
| Who is affected by the breach?                        | <ul style="list-style-type: none"> <li>• Individual or organisation?</li> <li>• How many individuals or organisations are affected?</li> <li>• Does the individual's personal circumstances put them at particular risk of harm?</li> </ul>                                                                                                                                                                                                                                                                                |

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What was the cause of the breach?                                        | <ul style="list-style-type: none"> <li>Human error, systems failure, or malicious or criminal act?</li> <li>Does it expose an underlying systemic vulnerability?</li> <li>Was it a one-off incident or has it occurred before?</li> </ul>                                                                                                                                                                                                                                                     |
| What is the foreseeable harm to affected individuals or organisations?   | <ul style="list-style-type: none"> <li>What is the possible use(s) for the personal information/data?</li> <li>Who is in receipt of the personal information/data?</li> <li>What is the risk of further access, use or disclosure?</li> <li>What harm has occurred?</li> <li>What steps have been taken to contain the breach?</li> <li>Has the personal information/data been recovered?</li> <li>Is the personal information/data encrypted or otherwise not readily accessible?</li> </ul> |
| Guidance issued by the Privacy Commissioner about eligible data breaches | IPC Guidelines on the assessment of data breaches under Part 6A of the PPIP Act.                                                                                                                                                                                                                                                                                                                                                                                                              |

The reporting form will be submitted to the Director for approval. The manager of the relevant business unit will be responsible for the implementation of approved actions and recommendations.

Within seven (7) working days, the Director will review the initial assessment of the manager and determine whether to approve 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 PPIP Act requires the assessment as to whether the incident is an eligible data breach to be carried out **within 30 calendar days** after a reasonable suspicion is formed that a data breach has occurred. The assessment must be carried out expeditiously. This means that the 30 calendar days should be treated as the maximum timeframe to complete the assessment. If an assessment cannot be completed within the legislated 30-day timeframe, the Director must seek an extension to the assessment period from the Commissioner.

The Privacy Commissioner must be notified of any extensions sought to the assessment period, including details as to:

- the date the assessment commenced
- the specific extension period.

## Step 2: Notification

### 2.1 Where the breach is an eligible data breach

If it is decided that an eligible data breach has occurred, the notification process under the MNDB Scheme is triggered (see Part 6A, Division 3 of the PPIP Act).

The ADC must take the following steps as part of this process:

- Immediately notify the Privacy Commissioner of the eligible data breach, using the approved form.

- Take reasonable steps to notify affected individuals as soon as practicable, unless one of the exemptions set out in Part 6A, Division 4 of the PPIP Act applies.

The Director is responsible for coordinating the notification process in this Policy.

### Privacy Commissioner

The Director will submit a briefing note to the Commissioner for approval on the eligible data breach, which includes details of the information that will be provided to the Privacy Commissioner as part of the notification.

This Policy sets a target for notification of the Privacy Commissioner **within one (1) working day** of the ADC's decision that an eligible data breach has occurred, but this timeframe is subject to practical factors. The notification to the Privacy Commissioner is to be made using the approved form 'Data Breach Notification to the Privacy Commissioner' on the IPC's website.

Any information that was not provided to the Privacy Commissioner as part of the immediate notification must be provided using the approved form. This is to occur following notification of affected individuals, or (if an exemption under Part 6A, Division 4 of the PPIP Act applies) following the Commissioner determining that an exemption applies.

### Affected individuals

An 'affected individual' is defined under section 59D of the PPIP Act as an individual:

- to whom the information subject to data breach relates; and
- who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.

As part of mitigating the data breach, you may have made contact with affected individuals to advise them of the potential for harm. This section relates to the formal notification of the data breach.

Before proceeding with notifying affected individuals, a determination should be made as to whether an exemption set out in Part 6A, Division 4 of the PPIP Act applies to the eligible data breach. The exemptions are:

- 1) Multiple public sector agencies are involved in the same eligible data breach and one of those agencies undertakes to notify affected individuals of the breach.
- 2) The Commissioner reasonably believes that notifying affected individuals of the eligible data breach would be likely to prejudice matters such as an ongoing investigation that could lead to the prosecution of an offence, or proceedings before a court or tribunal.
- 3) The agency has taken certain action to mitigate:
  - the harm done by an eligible data breach such that a reasonable person would conclude that the unauthorised access to, or disclosure of, personal information would not be likely to result in serious harm to an individual, or
  - the loss of personal information such that there is no unauthorised access to, or unauthorised disclosure of, the information,

- 4) Notifying affected individuals would be inconsistent with secrecy provisions.
- 5) The Commissioner reasonably believes notification of affected individuals would create a risk of harm to an individual's health or safety.
- 6) The Commissioner reasonably believes notification would worsen the agency's cyber security or lead to further data breaches.

If an exemption applies, the ADC may not be required to notify affected individuals for a particular matter.

The Director, in conjunction with advice from the relevant business unit, may seek an exemption from the Commissioner from notifying affected individuals if one or more of the above circumstances are relevant.

All eligible data breaches must be notified to the NSW Privacy Commissioner. Details of any approved exemptions from notification of affected individuals must be provided to the Privacy Commissioner.

If an exemption does not apply, affected individuals should be notified as soon as practicable after the ADC decides that an eligible data breach has occurred. This Policy sets a target for notification of affected individuals **within five (5) working days** of the ADC's decision that an eligible data breach has occurred, but this timeframe is subject to practical factors.

The method of notifying affected individuals will depend on the type and scale of the breach, and practical issues such as whether each affected individual can be contacted. Where the affected individual(s) can be contacted, they should be notified directly (for example, telephone, email or letter).

Where all individuals affected by an eligible data breach cannot be notified (for example, due to the size of the breach, or because their contact details are unknown and cannot reasonably be obtained), the ADC, with approval from the Commissioner, will issue a public notification on its website and the matter will be recorded on the ADC's Public Notification Register for a period of 12 months on the ADC's website.

The ADC must provide the Privacy Commissioner with information about how to access the notification on the Public Notification Register as soon as practicable after the notification is published.

Section 590 of the PPIP Act sets out the information that must be included in a notification to affected individuals, if it is reasonably practicable to do so:

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred (for example, unauthorised disclosure, unauthorised access, loss of information)
- the personal information that was breached

- the amount of time the personal information was disclosed for
- actions that have been taken or are planned to ensure the information is secure, or to control or mitigate the harm done to the individual
- recommendations about the step the individual should take in response to the breach
- information about how to make complaints or seek review of the agency's conduct
- the name of the agencies that were the subject of the breach
- contact details for the agency or the person nominated by the agency as the point of contact.

### ID Support NSW

Where a data breach involves the loss or compromise of proof of identity documents (such as driver licence, birth certificate), it is appropriate to include the contact details and general information about the support/services offered by [ID Support NSW](#) in the notification to any affected individuals, which includes:

- giving advice on compromised identification documents and how to restore the security of identity
- how to keep personal identity information safe
- options for additional support and counselling services.

### Communication with external bodies

The ADC will consider whether reporting the data breach to an external body is required or appropriate. For example, whether the ADC is required by a contract/memorandum of understanding/agreement to notify the external body of a data breach, or whether the circumstances of the breach require the data breach to be reported to the external body.

This could include (but is not limited to):

|                                                                      |                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NSW Police/<br>Australian Federal<br>Police                          | Where the ADC suspects a data breach is a result of criminal activity.                                                                                                                                                                                                                        |
| DCJ                                                                  | Where the data breach relates to, or could have an impact on, DCJ's IT network.                                                                                                                                                                                                               |
| Cyber Security<br>NSW                                                | Where a data breach is a result of a cyber security incident.                                                                                                                                                                                                                                 |
| iCare                                                                | Nominal insurer who may approve the services of an external legal services provider and/or project manager to assist with managing the breach.                                                                                                                                                |
| IDCARE                                                               | IDCARE is Australia and New Zealand's national identity and cyber support service.                                                                                                                                                                                                            |
| ID Support                                                           | Providing advice to breached agencies for remediation pathways and response, coordinating whole-of-government activities, ID Support Advisors can provide case management services to affected individuals.                                                                                   |
| Office of the<br>Australian<br>Information<br>Commissioner<br>(OAIC) | Under the Commonwealth Notifiable Data Breaches scheme, any organisation or agency covered by the <i>Privacy Act 1988</i> (Cth) must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. |

## 2.2 Where the breach is not an eligible data breach

If a data breach is not an eligible data breach under the MNDB Scheme, the ADC may still consider notifying affected individuals of the breach on a case-by-case basis. While notification demonstrates the ADC's commitment to open and transparent governance, consideration should also be given as to whether notification may be counterproductive. For example, notifying an individual about a data breach that poses very little or no risk of harm can cause them unnecessary stress or harm.

### Step 3: Review and learn

All ADC business units are required to enter any data breach or suspected data breach into the ADC Data Breach Register. The register will be regularly audited for quality assurance purposes and to gauge consistency of decision-making across the ADC.

The ADC will review and learn from any data breach, to consider and implement measures that could strengthen the ADC's personal information security and handling practices and prevent similar incidents occurring in the future. The review will be undertaken by the appropriate business area. For example, if the data breach was caused by human error, the business unit from which the breach arose should undertake the review; if the data breach was caused by a DCJ systems failure, the IT team should undertake the review.

Depending on the nature of the data breach, this step may be completed as part of the mitigation process or as part of the overall assessment of the ADC's response to the data breach.

Where appropriate, a post-incident review may include:

- examining the cause of the breach, including identifying any weaknesses in information handling and/or systems technology that gave rise to the breach
- consideration of whether the breach was a systemic problem or an isolated incident
- reviewing and improving IT or physical security requirements, including auditing requirements
- assessing IT systems for system vulnerabilities and taking preventive measures to negate the risk of a data breach recurring
- making appropriate changes to ADC policies, procedures, and, where appropriate, contracts, including updating this policy
- identifying further learning and training opportunities
- gathering feedback from key stakeholders engaged in responding to the breach to identify lessons learned from the breach response.

Any recommendations to implement remedial action or updates following a review are to be approved by the Director and documented in the ADC's Data Breach Register.

ADC staff will be notified of any updates or changes to policies and procedures relating to data breaches.

All post-incident communications must be limited to those with a legitimate need to know. Forwarding of sensitive information regarding the breach must be done with care, ensuring non-essential information is removed and/or redacted to prevent further data breaches.

## Related documents

- ADC Privacy and Information Management Framework
- Information Security Management System (ISMS) Information Security Policy and Framework (Intranet)

## Relevant legislation

- *Privacy and Personal Information Protection Act 1998*
- *Government Information (Public Access) Act 2009*
- *Health Records and Information Privacy Act 2002*

## Document information

| Category           | Description                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title              | ADC Data Breach Policy                                                                                                                                        |
| Date of effect     | September 2026                                                                                                                                                |
| Next review date   | September 2027<br><br>The review will be conducted earlier if any legislative, administrative or systemic changes affect the ADC's response to a data breach. |
| Document reference | ADCDOC26/100016                                                                                                                                               |
| Approval           | Commissioner                                                                                                                                                  |
| Version            | 1.0                                                                                                                                                           |

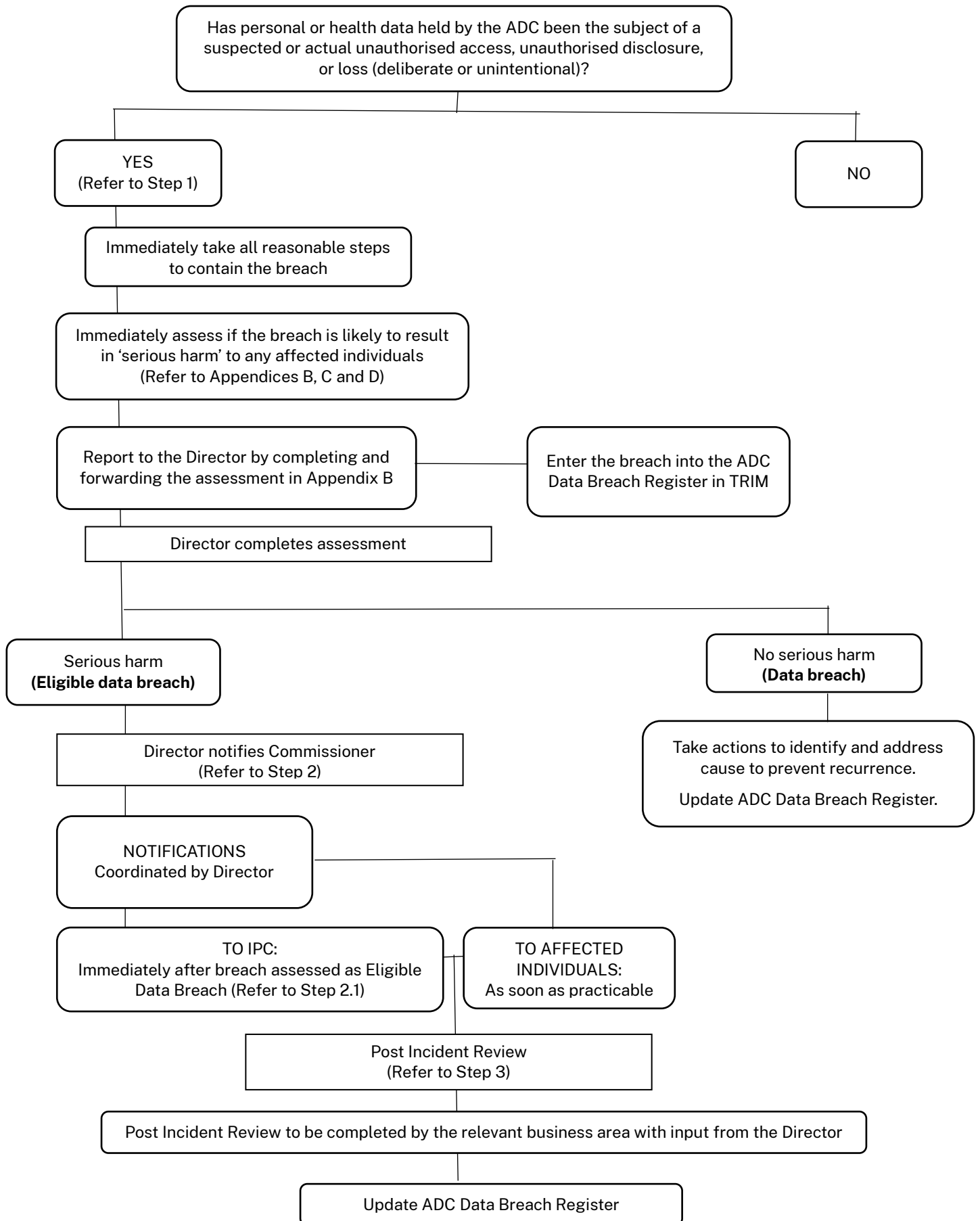
### NSW Ageing and Disability Commission

[www.adc.nsw.gov.au](http://www.adc.nsw.gov.au)

(02) 4904 7500

PO Box 40  
Parramatta NSW 2124

## Appendix A: Flowchart



## Appendix B: Reporting form and assessing serious harm

| Information regarding the data breach<br>(If available at time of report)                                                                                | Responses to be completed by Business Unit |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>Do not include sensitive, personal, or confidential information in this report.</b>                                                                   |                                            |
| <b>Key contacts</b>                                                                                                                                      |                                            |
| Contact details and position titles of staff in the business unit that are managing the <b>data breach</b> .                                             |                                            |
| <b>The data breach</b>                                                                                                                                   |                                            |
| Date and time the <b>data breach</b> occurred.                                                                                                           |                                            |
| Date and time the <b>data breach</b> was discovered.                                                                                                     |                                            |
| Type of personal and or health information involved (for example, specific personal information, client names, dates of birth).                          |                                            |
| Cause of the <b>data breach</b> (for example, lost laptop, hard copy documents, email sent to wrong person).                                             |                                            |
| ADC information, systems, and or assets impacted by the <b>data breach</b>                                                                               |                                            |
| Is the <b>data breach</b> a <i>cyber incident</i> , for example, an ADC database was compromised by a threat actor? (If yes, include details).           |                                            |
| Is there suspected misconduct by an employee, approved user, or contractor?                                                                              |                                            |
| <b>Assessing serious harm</b>                                                                                                                            |                                            |
| Sensitivity of the personal information involved in the <b>data breach</b> , for example, health information, sexual orientation.                        |                                            |
| Has personal information been lost, reproduced, or published (for example, on the internet) or has someone been provided with a copy of the information? |                                            |
| How many people (if known) had or currently have access to the personal information following the <b>data breach</b> ?                                   |                                            |
| Amount of time the personal information remained unprotected or accessible? Is the information                                                           |                                            |

|                                                                                                                                                                                                                                                                                                                                |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| still unprotected?                                                                                                                                                                                                                                                                                                             |  |
| Total (estimated) number of individuals affected                                                                                                                                                                                                                                                                               |  |
| Are the affected individuals from a vulnerable cohort? If so, provide further details.                                                                                                                                                                                                                                         |  |
| Are the individuals easily identifiable from the personal information subject to the <b>data breach</b> ?                                                                                                                                                                                                                      |  |
| <b>Mitigation of harm</b>                                                                                                                                                                                                                                                                                                      |  |
| Any immediate steps available, or taken, to contain the <b>data breach</b> ? For example, recalling the email, contacting the recipient and asking for it to be deleted (including deletion from their deleted items), or file to be returned.<br>For email data breaches, see <a href="#">Factsheet</a> for more information. |  |
| Any discussion with Cyber Security expert to identify immediate response steps?                                                                                                                                                                                                                                                |  |
| If applicable, Cyber Security expert's suggestions for reducing the scale and impact of the data breach (to minimise any harm to affected individuals or to the agency).                                                                                                                                                       |  |
| Whether any individuals affected by the data breach have been notified or are aware?                                                                                                                                                                                                                                           |  |
| <b>Stakeholders</b>                                                                                                                                                                                                                                                                                                            |  |
| Any other public sector agencies impacted by the <b>data breach</b> ? (List the agencies).                                                                                                                                                                                                                                     |  |
| Is a contractor involved? (If yes, provide a copy of any contract, data management processes and a nominated contract representative for the contractor).                                                                                                                                                                      |  |
| Any other key stakeholders who should be involved (if not covered in the information above)?                                                                                                                                                                                                                                   |  |
| <b>Additional information</b>                                                                                                                                                                                                                                                                                                  |  |
| Any other relevant information not provided above?                                                                                                                                                                                                                                                                             |  |

| Business unit's preliminary assessment of the data breach                                                            |  |
|----------------------------------------------------------------------------------------------------------------------|--|
| Has the business unit (at this time) assessed the <b>data breach</b> as an <b>eligible data breach</b> ? If so, why? |  |
| <b>Name and title of assessor</b>                                                                                    |  |
| <b>Date</b>                                                                                                          |  |
| Director's assessment of the data breach                                                                             |  |
| Director's assessment                                                                                                |  |
| <b>Name</b>                                                                                                          |  |
| <b>Date</b>                                                                                                          |  |

## Appendix C – Privacy risk matrix

### ADC – Privacy risk matrix

|                                              | Consequence                                                                                                                                                                                                                                         |                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                           |                                                                                                                                                                                                               |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | Insignificant                                                                                                                                                                                                                                       | Minor                                                                                                                                                                                                                  | Moderate                                                                                                                                                                                                                                                            | Major                                                                                                                                                                                                     | Significant                                                                                                                                                                                                   |
| Likelihood of risk after initial containment | Insignificant reputational damage, emotional or physical harm, and/or financial loss for an individual/s.                                                                                                                                           | Limited reputational damage, emotional or physical harm, and/or financial loss for an individual/s.                                                                                                                    | Reputational damage, emotional or physical harm, and/or financial loss for an individual/s.                                                                                                                                                                         | Major reputational damage, emotional or physical harm, and/or financial loss for an individual/s.                                                                                                         | Severe reputational damage, emotional or physical harm, and/or financial loss for an individual/s.                                                                                                            |
|                                              | Insignificant reputational damage/loss of trust in the ADC.<br><br><i>Example:</i><br>Information that is disclosed is already in the public domain or it may be difficult to identify the individual. No health or sensitive information involved. | Limited reputational damage/loss of trust in the ADC.<br><br><i>Example:</i><br>Disclosure results in limited/no risk of harm impacting a small number of individuals. No health or sensitive information is involved. | Reputational damage/loss of trust in the ADC.<br><br><i>Example:</i><br>Disclosure results in a risk of harm impacting any number of individuals OR a limited/no risk of harm impacting a large number of individuals. May include health or sensitive information. | Major reputational damage/loss of trust in the ADC.<br><br><i>Example:</i><br>Disclosure results in a serious risk of harm impacting any number of individuals. Includes health or sensitive information. | Severe reputational damage/loss of trust in the ADC.<br><br><i>Example:</i><br>Disclosure results in very serious risk of harm impacting any number of individuals. Includes health or sensitive information. |
| Almost Certain                               | Low                                                                                                                                                                                                                                                 | Medium                                                                                                                                                                                                                 | High                                                                                                                                                                                                                                                                | Critical                                                                                                                                                                                                  | Critical                                                                                                                                                                                                      |
| Likely                                       | Low                                                                                                                                                                                                                                                 | Medium                                                                                                                                                                                                                 | High                                                                                                                                                                                                                                                                | High                                                                                                                                                                                                      | Critical                                                                                                                                                                                                      |
| Possible                                     | Low                                                                                                                                                                                                                                                 | Medium                                                                                                                                                                                                                 | Medium                                                                                                                                                                                                                                                              | High                                                                                                                                                                                                      | High                                                                                                                                                                                                          |
| Unlikely                                     | Low                                                                                                                                                                                                                                                 | Low                                                                                                                                                                                                                    | Medium                                                                                                                                                                                                                                                              | Medium                                                                                                                                                                                                    | High                                                                                                                                                                                                          |
| Rare                                         | Low                                                                                                                                                                                                                                                 | Low                                                                                                                                                                                                                    | Low                                                                                                                                                                                                                                                                 | Medium                                                                                                                                                                                                    | High                                                                                                                                                                                                          |

## Appendix D: Personal information risk matrix

| Priority risk group                                | 1. Personal safety                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2. Personal identity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 3. Personal reputation                                                                                                                                                                                                                                                                                                                 | 4. Organisational integrity                                                                                                                                                                                                                                         | 5. Other                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Risk type</b>                                   | Immediate risk to life and/or ongoing harm                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Evasion of justice and fraud                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Personally sensitive                                                                                                                                                                                                                                                                                                                   | Damaging to the ADC, NSW Government or commercial partners                                                                                                                                                                                                          | Risks not covered in groups 1-4                                                                                                                                                                                                                                                                                                                                              |
| <b>Consequence (Risk matrix)</b>                   | Significant                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Major                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Moderate                                                                                                                                                                                                                                                                                                                               | Minor                                                                                                                                                                                                                                                               | Insignificant                                                                                                                                                                                                                                                                                                                                                                |
| <b>Examples of information potentially exposed</b> | <p>Persons at risk due to domestic / social situation:</p> <ul style="list-style-type: none"> <li>Justice records/ information</li> <li>At risk assessment, Ward of State, out-of-home care or Court Orders</li> <li>AVOs or juvenile justice records</li> <li>Survivors of family and domestic violence, including suppressed address</li> </ul> <p>Persons at risk due to:</p> <ul style="list-style-type: none"> <li>Detailed and identifiable medical or patient history of sensitive nature</li> </ul> | <p>Persons with personal identification and location:</p> <ul style="list-style-type: none"> <li>Full name +</li> <li>Address (phone number, email address or physical / mailing address)</li> </ul> <p>+</p> <ul style="list-style-type: none"> <li>Date of birth</li> </ul> <p>Also consider other vulnerabilities:</p> <ul style="list-style-type: none"> <li>Password reset questions</li> <li>Medicare number</li> <li>Passport number</li> <li>Birth / death / marriage certificate</li> <li>Tax file number</li> <li>Credit card number</li> <li>P card number</li> <li>Immigration or visa details</li> <li>Bank account details</li> <li>Driver licence details</li> </ul> | <ul style="list-style-type: none"> <li>Private employer or high-profile individuals being blackmailed, publicly embarrassed or defamed</li> <li>Reputational / industrial risk to the department</li> <li>Criminal history including police checks</li> <li>Practitioner reviews</li> <li>Investigation reports and results</li> </ul> | <ul style="list-style-type: none"> <li>In confidence material</li> <li>Internal correspondence</li> <li>Internal information on policy or financials</li> <li>Cabinet level information</li> <li>Standing orders</li> <li>Legally privileged information</li> </ul> | <ul style="list-style-type: none"> <li>Other risks not described in risk group 1-3 e.g., psychological distress</li> <li>Documents without PII</li> <li>Photos without identification</li> <li>Information that is no longer sensitive, or is now publicly available</li> <li>ABN of a sole trader</li> <li>Vehicle registration details</li> <li>Driving records</li> </ul> |