audit office
OF NEW SOUTH WALES

Data Breach Management Policy

Date: 28 November 2023

contents

1. Policy statement

In carrying out its statutory functions, the Audit Office has access to a significant amount of information. Some of this is merely sighted during the course of an audit or other function, while other data forms records retained by the Audit Office. Importantly, the information that the Audit Office holds includes sensitive information that must be protected in certain ways, such as personal and health information, and official government information.

Data breaches need to be responded to quickly, and on a case-by-case basis depending on the nature and context of the breach. A data breach can be due to one or several factors, such as human error or a cyber security incident.

The purpose of this Data Breach Management Policy (the Policy) is to provide guidance to staff and contractors of the Audit Office in the event of a data breach originating from the Audit Office, or third parties contracted with the Audit Office.

This Policy aims to ensure that data breaches are contained, assessed, and responded to, as quickly as possible. It also aims to ensure that our responses are effective in minimising risks to affected parties and the Audit Office and are consistent with our legal obligations, including mandatory notification requirements.

Detail on the steps to take when responding to data breaches, including relevant templates, are located in the Data Breach Response Procedure.

The Audit Office has a low-risk appetite with respect to the management of data breaches.

2. Scope

This Policy applies to all permanent and temporary staff and the contingent workforce employed by the Audit Office.

This Policy covers requirements for responding to all types of data breaches as defined in section 3, including but not limited to those where mandatory notification requirements apply.

Note on third-party providers

The Audit Office has arrangements with third parties that hold or manage information on our behalf. Arrangements include requirements that third party providers comply with privacy laws and provide assurances to us with respect to notifying and cooperating with us in the event of a data breach. Our Third Party Security Policy establishes control and mitigation processes to minimise risks associated with potential security breaches. Our Audit Office's Audit Service Provider (ASP) Manual includes requirements on audit service providers in the event of a data breach.

2.1 Legislative context and types of information

There are a number of legal requirements when it comes to the Audit Office's handling of information and our responses to data breaches. The requirements depend on the type(s) of information breached.

Personal and health information

Personal Information is defined in section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) as, information or an opinion about an individual whose identity is apparent or can be reasonably ascertained.

Under the PPIP Act, the Audit Office is required to manage personal information in accordance with the Information Protection Principles.

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

Under the HRIP Act the Audit Office is required to manage health information in accordance with the Health Privacy Principles.

A data breach involving personal (including health) information is likely to require a non-mandatory data breach notification to the affected individuals under this Policy and may also be an '**eligible data breach'** under the PPIP Act's Mandatory Notification of Data Breach Scheme. An eligible data breach is where there is a likely risk of serious harm to individuals affected by the breach of personal information. See section 3.2 of this Policy and for guidance on the definition of eligible breaches.

For further information on our obligations to protect personal and health information, refer to the Audit Office's Privacy Management Plan.

Personal information – tax file number(s)

Under the *Privacy Act 1988* (Cth), the Audit Office is required to notify affected individuals and the Office of the Australian Information Commissioner where a tax file number(s) is the subject of a data breach and where the breach is likely to result in serious harm to an individual.

A tax file number breach is also likely to be an eligible breach and require mandatory notifications to affected individuals and the Privacy Commissioner NSW under the PPIP Act's Mandatory Notification of Data Breach Scheme.

Official information

Most information that the Audit Office holds will be official information that has been created by and that belongs to the Audit Office (corporate information), or information collected through our audit-related functions.

Although breaches of official information do not trigger the statutory mandatory notification schemes – unless it also involves personal information where it is likely there is a serious risk of harm to affected individuals (as above) – official information is likely to be classified as 'sensitive' and require protections. In particular:

- **'Audit-related' information:** Section 38 of the *Government Sector Audit Act 1983* and section 425 of *the Local Government Act 1993* require the preservation of secrecy of "all matters and things" that comes to the knowledge of any staff member as a result of exercising a function under the respective Acts, such as conducting an audit.
- **Other confidential information:** The Audit Office holds confidential information such as Cabinet-in-Confidence and Legal Professional Privilege information, which are sensitive and may also be protected under our secrecy provisions if collected or received as part of an audit.

Official records of the Audit Office that do not fall into the above categories may nonetheless be classified as sensitive. Breaches of official information are likely to require a non-mandatory data breach notification under this Policy.

Refer to the Audit Office's Information Classification and Labelling Policy for more information.

3. Types of data breaches

A data breach occurs when an incident has caused or has the potential to cause unauthorised access to, disclosure of, or loss of information (digital or hard copy) belonging to or held by the Audit Office.

3.1 Data breaches in general

Data breaches can involve:

Unauthorised access such as cyber-attacks, or employees intentionally opening a file containing information to which they don't have access.

Unauthorised disclosure such as human or technical errors, like sending an email to the wrong recipient or uploading incorrect information to an external file share site or our website.

Loss of information such as the accidental loss of a paper record, work device, or a cyber-attack resulting in the loss of information.

3.2 Eligible data breaches

An eligible data breach involves personal information where a reasonable person would conclude that the access or disclosure of information due to the breach is likely to result in serious harm to an individual to whom the information relates.

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. Serious harm is 'likely' when it is more probable than not, not merely possible.

Serious harm can include physical, financial, material, emotional, psychological, or 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 impact of the harm can vary from person to person, but may include:

- financial loss through fraud
- a likely risk of physical or psychological harm
- identity theft, which can affect your finances and/or credit record
- serious harm to an individual's reputation.

See Appendix A for more guidance on identifying the likely risk of serious harm for eligible breaches.

4. Types of notifications

4.1 Mandatory notifications (of 'eligible breaches')

The Audit Office has an obligation under Division 3 of the Mandatory Notification of Data Breach (MNDB) Scheme (Part 6A of the PPIP Act) to notify certain parties, such as affected individuals or agencies, and oversight bodies, of an eligible data breach. Relevant oversight bodies are the NSW Information and Privacy Commission and Office of the Australian Information Commissioner (OIAC).

There are requirements under Section 59M and 59O of the PPIP Act around the information that must be provided to notifiable parties about the breach and reported on to the relevant oversight bodies.

4.2 Non-mandatory notifications

The Audit Office may decide to notify an affected individual and/or agency about a data breach. This can assist them and us to take steps to reduce risks related to the breach. It may also be considered appropriate to notify individuals and/or agencies as a courtesy.

5. Preparing for a breach

The Audit Office has two nominated Privacy Officers, whose role it is to raise awareness of and manage day to day privacy matters, and who are involved in coordinating the response to data breaches.

The Audit Office has a Privacy Management Plan, as required under the PPIP Act. In addition, the Audit Office has established a range of policies and processes that are relevant to minimising the risk of data breaches and/or enabling effective responses. These include:

- Code of Conduct
- ICT Acceptable Use Policy
- Identity and Access Management Policy
- Information Classification and Labelling Policy
- Mobile Device and Remote Working Policy
- Office Access Policy
- Secure Deletion and Disposal Policy
- Third Party Security Policy.

The Audit Office utilises an Audit Communication Portal (ACP) to enhance security measures to protect audit information, and to provide one centralised location for the exchange of this information to occur.

The Audit Office has pop-up warnings in place on all staff and official email accounts to alert users when an email containing an attachment is about to be sent to an external party – providing them with an opportunity to check the recipients and content before the email is transmitted.

Cyber training is provided to Audit Office staff annually. The Audit Office will continue to review the training needs of staff with respect to data breaches and provide training in reporting, managing, and responding to data breaches.

6. Roles and responsibilities in responding to breaches

All Audit Office employees have a responsibility for immediately reporting a suspected data breach in accordance with this Policy, and supporting containment, response and reporting activities.

The **Deputy Auditor-General**:

- is responsible for oversight of data breach management, including the implementation of this Policy and delegated decisions in response to eligible breaches.
- following a notification of an actual or suspected data breach
  - assigns the Response Coordinator
  - approves the assessment of whether a breach is an ‘eligible breach’ that triggers mandatory notification requirements
  - approves the scope and approach to non-mandatory data breach notifications.

The **Interim Response Coordinator** is a Director (or equivalent) responsible for the area where the data breach originated and is responsible for taking the initial steps to contain the breach (as soon as practicable and within 24 hours) and for notifying the:

- Deputy Auditor-General
- Chief Information Officer
- Information & Security Architect

- Executive Director – Professional Services
- Executive Director – Corporate, Experience and Strategy
- Privacy officers: Director, Governance (Legal) and Governance Officer
- relevant Assistant Auditor-General or Executive Director in the relevant branch
- Service Desk.

The **Response Coordinator** is responsible for coordinating the implementation of response steps 2, 3, 4 and 5. This is done with support of the Data Breach Response Team, advice from the Governance team, and the oversight of the Deputy Auditor-General. Further details of each of these steps are in section 7 of this Policy, included in the Data Breach Response Plan.

The Response Coordinators must prepare a brief on the breach and response to the Office Executive. The template for this brief is in the Data Breach Response Plan.

The **Data Breach Response team** consists of the:

- Relevant Branch/Neighbourhood head
- Chief Information Officer
- Privacy Officer - Governance Officer or Director Governance (Legal), or both, depending on the nature and context of the breach.

Other staff may form part of the Data Breach Response team depending on the nature and context of the breach.

The **Office Executive** support the Deputy Auditor-General by overseeing the Audit Office's response to data breaches and determining steps to prevent future breaches.

Privacy Officers (Director, Governance (Legal) and Governance Officer), have a role in:

- supporting the coordination of the response
- ensuring that accurate and timely reporting is provided to the Office Executive
- providing advice to the Deputy Auditor-General on whether a breach is an eligible breach, and other risks or issues related to the breach, response and notification requirements
- reviewing information for mandatory data breach notifications to individuals, agencies, NSW Privacy Commissioner and the OIAC
- preparing information for statutory reporting requirements.

7. Reporting and responding to a data breach

There is no single method of responding to a data breach. Data breaches must be dealt with swiftly on a case-by-case basis, by undertaking an assessment on the nature of the breach and type of data involved and using this information to evaluate the associated risks to determine the appropriate course of action.

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

Step 1. Make all reasonable efforts to ***contain*** the breach and make an initial report to relevant internal parties.

Step 2. ***Assess*** and ***determine*** the nature of the breach and type of data involved.

Step 3. ***Evaluate*** the associated risks.

Step 4. Identify who to ***notify*** – confirm any mandatory notification requirements, consider non-mandatory notifications to other parties.

Step 5. ***Prevent*** a repeat.

Each step is set out in further detail below.

7.1 Step 1. Contain the breach

Make all reasonable efforts to contain the breach and make an initial report to relevant internal parties.

The Audit Office will prioritise containment of a suspected or actual data breach. All reasonable efforts must be taken to contain the breach and mitigate any resulting harm.

Initial containment action

Containment actions can include:

- shutting down the system that has been breached
- revoking or changing access codes or passwords
- restricting access rights to Audit Office systems and data
- contacting third-party recipients to request any data that they received in error (e.g., email or attachment) has been permanently deleted, and requesting written confirmation of this.

Informing internal parties

If it is suspected that a data breach has occurred any employee of the Audit Office must immediately report the suspected breach to their People Manager and relevant Director, if different, so that the Interim Response Coordinator can be nominated. Similarly, third-party service providers must immediately notify the Director or Executive Manager responsible for managing the contract.

The Interim Response Coordinator must in turn inform the Deputy Auditor-General of the data breach or suspected data breach as soon as practicably possible (no later than within 24 hours). When doing so, the Interim Response Coordinator should provide information about the nature and type of breach, and any initial containment action taken.

An internal ‘data breach notification’ group email has been established to enable the Interim Response Coordinator to rapidly and in a streamlined way notify the relevant officers and the Service Desk. The Service Desk is included in the internal ‘data breach notification’ email group so that any containment action under the Cyber Security Incident Management Policy can occur rapidly, if relevant.

In practice this means that the Interim Response Coordinator should email the data breach notification group PLUS the relevant Assistant Auditor-General or Executive Director in the branch where the breach occurred.

The Response Coordinator is appointed by the Deputy Auditor-General and is responsible for steps 2 to 5 below, with the support of the Data Breach Response Team.

In some circumstances, the Deputy Auditor-General may decide to call a meeting of the Crisis Management Team.

7.2 Step 2. Assess the breach

Assess and determine the nature of the breach and type of data involved.

The Response Coordinator makes an assessment of the data breach, determining the nature in which the breach occurred, the severity of the breach, the type of data affected (Auditee, Staff, or Corporate) and its sensitivity.

Depending on the context of the breach, the Response Coordinator should consider including additional Response team members as appropriate:

- Information and Security Architect
- Executive Director, Corporate, Experience and Strategy
- Executive Director, Professional Services
- Executive Director, Finance and Performance
- Director responsible for the auditee/audit
- Director, People and Culture
- Records Manager.

The Response Coordinator is responsible for completing the data breach response checklist, located in the Data Breach Response Plan.

7.3 Step 3. Evaluate the breach

Evaluate associated risks and determine remedial action.

To determine what other steps are needed, there must be clarity around the risks for harm associated with the data breach. Some types of data are more likely to cause serious harm if compromised. A combination of data will typically create a greater potential for harm than a single piece of data.

Factors to consider in evaluating the associated risks include:

- What type of data is involved in the breach?
- What is the (current and possible) extent of the breach? Have actions to contain the breach been successful?
- Who is affected by the breach? What is the foreseeable harm to the affected individual(s)/organisation(s)?
- What was the cause of the breach?

The Response Coordinator in consultation with the Privacy Officer and the Director Governance will assess whether the breach is an eligible breach that requires mandatory notifications. This advice will be provided to the Deputy Auditor-General for review and confirmation as part of Step 4 (below).

Take remedial action

The Response Coordinator, in consultation with the Data Breach Response Team, should consider if there are any additional steps (after the initial containment action) that can/should be taken to reduce any potential harm to individuals/organisations.

The Audit Office's Cyber Security Incident Management Policy sets out remediation actions that should be followed where the data breach is deemed to be caused by malicious parties, presents an ongoing risk, or is an active cyber incident.

7.4 Step 4. Identify who to notify

Confirm any mandatory notification requirements, consider other non-mandatory notifications.

The Audit Office recognises that notifications to individuals or organisations (such as other agencies) affected by a data breach can assist in mitigating risks or damage related to the breach. This is in addition to any initial notification or advice that occurs as part of initial containment activity.

The method of notifying affected parties will depend in large part on the type of data breach and the nature of the data involved. Whether the breach triggers a mandatory notification requirement or not, if notification is considered appropriate it should be done promptly to help to avoid or lessen any potential damage by enabling the affected parties to take steps to protect themselves.

If there is no mandatory requirement to notify affected parties, the Deputy Auditor-General will confirm the approach and scope of non-mandatory notifications.

If an eligible data breach has occurred, the notification process under Division 3 of the Mandatory Notification of Data Breach Scheme is triggered. In this case, the Deputy Auditor-General under delegation confirms the assessment of the breach as an eligible breach based on advice from the Privacy Officer and the Director Governance, in consultation with the Response Coordinator.

The Deputy Auditor-General, with support from the Privacy Officers, including the Director Governance, and relevant Response team members must:

- immediately notify the Privacy Commissioner about the breach
- determine whether an exemption applies in relation to an eligible data breach that may not require notification to affected individuals
- notify affected individuals or their authorised representative as soon as practicable (unless an exemption applies)
- provide additional information to the Privacy Commissioner (if required)
- update the Audit Office's public notification register with information about the eligible breach
- lodge a notification with the OIAC using the required form, for eligible breaches involving tax file numbers.

See section 8 of this Policy for further guidance on notifications.

Considerations for notification can also be found in the Data Breach Response Plan.

7.5 Step 5. Prevent a repeat.

Investigate causes and consider measures to prevent a reoccurrence.

The Data Breach Response Team will further investigate the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent a reoccurrence.

Preventative actions could include a:

- review of the Audit Office's IT systems and remedial actions to prevent future data breaches
- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

A report of the incident, including measures to prevent a reoccurrence, should be prepared and tabled at the next meeting of the Office Executive unless otherwise determined by the Deputy Auditor-General. See the template briefing note in the Data Breach Response Plan.

8. Guidance for notification

The following provides additional guidance in those instances where:

- a decision has been made that non-mandatory notification is appropriate and warranted to support affected parties to minimise the risk of harm, or if otherwise considered as a courtesy
- notification is mandatory
  - in the case if a data breach involving a tax file number
  - where the breach involves personal information and is classified as an eligible breach (as defined in section 3.2 of this Policy) and is likely to result in serious harm.

8.1 Non-mandatory notifications

In general, individuals and organisations (such as other agencies) affected by a breach should be notified as soon as practicable, after consultation with the Data Breach Response Team and approval of the Deputy Auditor-General.

Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

Affected parties should be notified directly – by telephone, letter, email or in person.

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.

See the Data Breach Response Plan for additional guidance on what to include in a notification.

8.2 Mandatory notifications

The Audit Office must notify the NSW Privacy Commissioner and affected individuals of eligible breaches i.e., data breaches involving personal information that is likely to result in serious harm.

Once the Deputy Auditor-General determines that an eligible data breach has occurred, they must:

- **immediately** notify the Privacy Commissioner using the form approved by the Privacy Commissioner, and
- **as soon as practicable** notify certain individuals.

A notification to individuals must include certain minimum details under the PPIP Act, such as information about the Audit Office, the data breach, the impact on individuals and mitigation steps available to individuals. Additional guidance on information to include in a mandatory notification can be located in the Data Breach Response Plan.

If the Audit Office is unable to notify or it is not reasonably practicable for any or all the affected individuals to be notified, the Audit Office will publish a notification and take all reasonable steps to publicise this notification. The notification will remain on the Audit Office's public notification register for a minimum period of 12 months. See our Communications Strategy (section 10) for further information.

Where required, notification of an eligible data breach involving a tax file number must also be lodged with the OAIC using the online form provided on the OAIC's website.

Exemptions from notification requirements for an eligible data breach

The Division 4 of the MNDB Scheme allows some exemptions from mandatory notification requirements to individuals.

It is possible that, depending on the context and the personal information breached, the Audit Office is not required to notify the individual, or is not required to provide all of the standard notification information items outlined in section 59N(1) of the PPIP Act.

For example, the Audit Office may not be required to notify an individual of an eligible data breach, or not be required to provide all of the information items, if:

- the breach involves more than one public sector agency (including the Audit Office) and another agency involved in the same breach notifies the Audit Office of the breach
- the notification would likely prejudice any investigation or legal proceedings
- the Audit Office successfully contains the breach and limits the likelihood that an individual will experience serious harm

- there are overriding secrecy provisions in other laws that prohibit or regulate the use or disclosure of the relevant information, such as secrecy protecting audit-related information under section 38 of the *Government Sector Audit Act 1983* (GSA Act).
- notification would create a serious risk of harm to an individual's health or safety
- notification would worsen the Audit Office's cybersecurity or lead to further data breaches.

The Deputy Auditor-General (under delegation), with advice from the Privacy Officers including the Director Governance, whether one of these exemptions to notifying individuals applies.

The PPIP Act does not establish exemptions from notifying the NSW Privacy Commissioner of eligible data breaches. Section 59M of the PPIP Act requires that the requested information is provided to the NSW Privacy Commissioner unless it is not reasonably practical to do so.

Notifications to Cyber Security NSW

For incoming technology cyber intrusions or breaches, the Chief Information Officer, should follow the Notification and Support guidance of section 6.1 of the Audit Office's Cyber Security Incident Management Policy, to determine if the Audit Office must notify Cyber Security NSW to ensure the integrity and protection of other state agencies who may be susceptible to similar attacks. This notification should not reveal the data breached but may reveal details on the means of the intrusion. Notifications can only be made with the approval of the Deputy Auditor-General under delegation.

9. Record keeping requirements

The Privacy Officer is responsible for maintaining appropriate records that provide evidence of how actual and suspected breaches are managed, including those not escalated to the response team or notified to the Privacy Commissioner.

In compliance with its obligations under the PPIP Act, the Audit Office maintains:

- a public data breach management policy,
- an internal register for eligible data breaches, and
- a public notifications register published on our website for all eligible data breaches.

The Audit Office also maintains an internal register of all data breaches.

10. Communication strategy

The Executive Director, Corporate, Experience and Strategy will be responsible the coordinating the implementation of public communications issued under this Policy, such as publicizing the notification of an eligible data breach to affected individuals.

The Audit Office's Business Continuity Plan contains a crisis communications strategy and template for messaging external stakeholders in crisis situations, such as cyber security incidents.

11. Contact point

Any inquiries concerning the Policy, or its application should be directed to the Audit Office's Privacy Officer by sending an email to governance@audit.nsw.gov.au.

12. Review

This Policy will be reviewed annually in the absence of any significant changes or more frequently where required taking into account legislative or organisational changes, risk factors and consistency with other policies.

Appendix A – Guidance for identifying a likely risk of serious harm (eligible data breaches)

The risk of serious harm must be assessed on a case-by-case basis. Each data breach will be different. Under the PIPP Act and for the purposes of this Policy, an eligible data breach involves personal information where the breach is likely to result in serious harm for individuals to who the breach relates.

The Audit Office collects a diverse range of information including personal information, commercial information and sensitive government information which may be the subject of a data breach. A risk of serious harm does not, however, depends not only on the type of information involved also other considerations related to the nature and scope of the breach.

Harms that can arise as a result of a data breach are context-specific and will vary based on:

- type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- level of sensitivity of the personal information accessed, disclosed or lost
- amount of time the personal information was exposed or accessible, including prior to the discovery of the breach
- circumstances of the individuals affected and their vulnerability or susceptibility to harm
- circumstances in which the breach occurred
- actions taken by the agency to reduce the risk of harm following the breach.

What is serious harm?

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of harm could be an outcome of a data 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.

While mere irritation or annoyance does not in itself amount to serious harm, emotional or psychological impacts of a data breach can amount to serious harm if they are severe.

When is a breach 'likely to result' in serious harm?

Whether a data breach is 'likely to result' in serious harm is an objective test to be determined from the perspective of a reasonable person and on the facts of the specific breach in question. In this context, the phrase 'likely to result' means that the risk of serious harm to an individual is more probable than not, rather than merely possible.

Serious harm does not need to be likely for all individuals to whom the breached information relates. A data breach will be an eligible data breach if serious harm is more likely than not for a single individual, or a subset of individuals involved in a breach.

Factors relevant to an assessment

The factors that may be relevant in assessing the likelihood and severity of harm are contextual to the specific type and form of the data breach. The factors listed below are not exhaustive, and whether there is a risk of serious harm arising from a data breach must be assessed based on the facts and context of each individual breach.

- The types of personal information involved in the breach
- The sensitivity of the personal information involved in the breach
- Whether the personal information is or was protected by security measures
- The persons who have, or may have, had access to the information
- Likelihood the person/s had malicious intent or capacity to circumvent security measures
- The nature of the harm that has occurred or may occur to the affected individuals
- The extent to which affected individuals may be particularly vulnerable to harm
- The ease with which information can be accessed and individuals identified.

Those responsible for considering the likely harm of an eligible data breach should also consider consulting with others in determining a recommendation as to whether serious harm is likely or not. The following officers provide some options for people who may be usefully consulted in considering the likely impact of a data breach:

- Executive Director, Professional Services
- Executive Director, Corporate, Experience and Strategy
- Chief Information Officer
- Privacy Contact Officer.

Breaches of tax files numbers will usually be treated as eligible breaches (if in doubt, assume that there is a serious risk of harm), and require mandatory notifications.

As noted in the Policy, any recommendation to notify requires approval by the Deputy Auditor-General.