audit office
OF NEW SOUTH WALES

Data Breach Management Policy

March 2021

INSIGHTS FOR BETTER GOVERNMENT

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.

The purpose of the 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). A data breach occurs when an incident has caused or has the potential to cause unauthorised access to Audit Office information (including information collected by the Audit Office from its auditees).

This includes the granting of access to information that a third party should not have access to – regardless of whether granting the access was unintentional, intentional, or consequential to another action.

The Policy sets out Audit Office procedures for managing a data breach so that the breach is contained, assessed and responded to, as quickly as possible. The Policy also includes considerations around notifying individuals or organisations whose data may be affected by the breach.

2. Scope

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

3. Responding to a data breach

The Director or Executive Manager of the area responsible for the breach is the Interim Response Coordinator. The Interim Response Coordinator is responsible for notifying the data breach or suspected data breach to the Deputy Auditor-General. Notification must be made to the Deputy Auditor-General as soon as practically possible (and no later than within 24 hours).

The Deputy Auditor-General will nominate a Response Coordinator (which may be the Interim Response Coordinator or an alternative member of staff) appropriate to the nature of the data breach to coordinate the Audit Office response to the data breach to ensure that it is managed in accordance with this Policy.

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

Step 1. ***Contain*** the breach and notify the Deputy Auditor-General
Step 2. ***Evaluate*** the associated risks
Step 3. Consider whether to ***notify*** affected individuals
Step 4. ***Prevent*** a repeat.

The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies. These steps are incorporated and explained in the following flowchart to guide action in the event of a data breach.

The data breach response checklist at Appendix A should be completed for all data breaches.

Data breach discovered or suspected

Discovered by, or notified to, staff or contractor.

Relevant Director or Executive Manager of the area responsible for the breach is the **Interim Response Coordinator**.

Is this a data breach?

A data breach occurs when an incident has caused or has the potential to cause unauthorised access to Audit Office information (including information collected by the Audit Office from its auditees).

If the incident is not a data breach, then no further action is required under this Policy.

If it is a data breach, proceed to Step 1: Contain the breach.

Step 1: Contain the breach

All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example, recover the information (including any copies), shut down the system that has been breached, suspend the activity that led to the breach, revoke or change access codes or passwords.

For all data breaches that occur via electronic means, the Interim Response Coordinator must notify the Service Desk who can begin activities to support containment in line with the Cyber Security Incident Management Policy.

Take the following steps to contain an email that has been sent or copied to the wrong recipient:

1. find out whether the recipient has read, printed or forwarded the email
2. confirm that the email has been deleted by the recipient
3. liaise with the recipient's IT department to confirm the email and any backups have been deleted from the system
4. notify the Deputy Auditor-General and the Service Desk as soon as possible.

Interim Response Coordinator to notify the Deputy Auditor-General

The Interim Response Coordinator must notify the Deputy Auditor-General of the data breach or suspected data breach as soon as practically possible (and no later than within 24 hours) including advice of any mitigation actions taken or proposed to be taken to contain the breach.

Note: Preliminary notification should be made as soon as possible and within the first few hours even if containment action is still being taken. Containment and any mitigation action should be completed within 48 hours of the breach and the Deputy Auditor-General updated when this is complete.

The Deputy Auditor-General will nominate a Response Coordinator (which may be the Interim Response Coordinator or an alternative member of staff) appropriate to the nature of the data breach to coordinate the Audit Office response to the data breach to ensure that it is managed in accordance with this Policy.

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

Notify the Data Breach Response team

The following officers form the Data Breach Response Team and must be notified and consulted throughout the response process:

- Relevant Branch/Neighbourhood head
- Chief Information Officer
- Information and Security Architect
- Privacy Contact Officer.

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

- Executive Director, Corporate Services
- Executive Director, Professional Services
- Director responsible for the auditee/audit
- Executive Manager, HR
- Records Manager.

Step 2: Evaluate the associated risks

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

The following should be considered in evaluating the risks:

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

Take remedial action

Are there any additional steps that can/should be taken to reduce any potential harm to individuals/organisations?

Follow the Cyber Security Incident Management Policy where the breach is:

- deemed to be caused by malicious parties
- an ongoing risk or
- an active cyber incident.

Step 3: Consider notifying affected individuals/organisations

If the data breach creates a real risk of serious harm* to an individual or organisation, the affected individuals or organisations should be notified. Prompt notification can help to avoid or lessen the damage by enabling the individual or organisation to take steps to protect themselves.

There are occasions where notification can be counterproductive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations. Consider the following when deciding whether to notify individuals/organisations about the data breach:

1. Are there any applicable legislative provisions or contractual obligations that require the Audit Office to notify affected individuals?
2. What type of information is involved?
3. What is the risk of harm to the individual/organisation? [*Appendix B provides guidance for assessment of 'serious harm']
4. Is this a repeated and/or systemic issue?
5. What risks are presented by the mode of the breach e.g. is it encrypted information or contained in a less secure platform e.g. email?
6. Does the breach relate to our audit functions and include audit related material?
7. What steps have been taken to date to avoid or remedy any actual or potential harm?
8. What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
9. Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause reputational damage (including humiliation or embarrassment) for the individual/organisation?

Note 1: The breach should not be notified to, or discussed with, any other individual or organisation other than those directly affected by the breach. To do so may constitute a breach of section 38 of the *Government Sector Audit Act 1983* and section 425 of the *Local Government Act 1993*. The Deputy Auditor-General may decide to notify the Information and Privacy Commission NSW (IPC) if appropriate. As a further exception, for incoming technology cyber intrusions or breaches, consideration should be made by the Chief Information Officer, in line with the Cyber Security Incident Management Policy, to 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.

Does the data breach involve a tax file number?

Yes

The Office of the Australian Information Commissioner (OAIC) must be notified if the data breach may result in serious harm to an individual.

No

Any decision to notify an individual/ organisation must have the approval of the Deputy Auditor-General.

Refer to section 4 below for further guidance on notification.

Step 4: Prevent a repeat

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:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices; or
- 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.

Note: See template briefing note for the Office Executive at Appendix C.

If the issue was a technology breach, ensure that the Office Executive briefing document/report to the Deputy Auditor-General is provided to the Service Desk to allow the security incident to be closed.

4. Guidance for notification

The following provides guidance in those instances where:

- notification is mandatory (in the case of a data breach involving a tax file number and where the breach is likely to result in serious harm) or
- a decision has been made that the notification is warranted as the data breach creates a risk of serious harm to the individual or organisation.

4.1 Who should notify

In general, the Audit Office should make notifications relating to data breaches by the Audit Office. This will ensure that the notification is made in accordance with the Audit Office's secrecy provisions and that feedback from affected individuals/organisations can be received directly. Where the data breach relates to auditee information, the Audit Office should liaise with the auditee and agree whether the Audit Office or the auditee should make the notification. Within the Audit Office, the Response Coordinator will make the notification. Notifications can only be made with the approval of the Deputy Auditor-General.

For incoming technology cyber intrusions or breaches, the Chief Information Officer, should follow the Notification and Support guidance of section 6.1 of the 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.

4.2 When to notify

In general, individuals/organisations affected by a breach should be notified as soon as practicable. 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.

4.3 How to notify

Affected individuals/organisations should be notified directly – by telephone, letter, email or in person.

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

Where notification to Cyber Security NSW is required, follow the guidance under the Notification and support section (6.1) of the Cyber Security Incident Management Policy.

4.4 What to say

The notification advice will be tailored to the circumstances of the particular breach but could include:

a) information about the breach, including when it happened
b) a description of what data or personal information has been disclosed
c) assurances (as appropriate) about what data has not been disclosed
d) a description of what measures have been taken to control or reduce the harm and the effectiveness of those measures
e) measures implemented to prevent future data breaches
f) contact details for the Audit Office for questions or requests for information
g) acknowledgement of their right to lodge a privacy complaint with the Privacy Commissioner.

A template notification letter is at Appendix D.

5. Roles and responsibilities

The **Deputy Auditor-General** is responsible for oversight of data breach management including the implementation of this Policy. The Deputy Auditor-General is to be notified of all actual or suspected data breaches and makes the decision regarding notification of data breaches

The **Interim Response Coordinator** is either a:

- Director or
- Executive Manager or equivalent in Professional Services and Corporate Services

responsible for the area where the data breach originated. The Interim Response Coordinator is responsible for taking the initial steps to contain the breach and for notifying the Deputy Auditor-General.

The **Response Coordinator** is appointed by the Deputy Auditor-General and is either the Interim Response Coordinator or another appropriate member of staff.

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

- Relevant Branch/Neighbourhood head
- Chief Information Officer
- Information and Security Architect
- Privacy Contact Officer.

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

6 Legislative context

Under the *Privacy Act 1988* (Commonwealth), the Audit Office is required to notify affected individuals and the OAIC 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. Outside of this, there are currently no mandatory requirements governing the management of data breaches in NSW government agencies. However, the IPC recommends that NSW agencies adopt a voluntary data breach notification policy. The adoption of a voluntary data breach notification policy has been approved by the Office Executive and this Policy is consistent with the guidance provided by the IPC on data breach management and is largely based on the IPC Data Breach Policy (June 2020).

This Policy should also be read in the context of specific requirements relating to the management of information by the Audit Office.

Section 38 of the *Government Sector Audit Act 1983* and section 425 of the *Local Government Act 1993* require the preservation of secrecy. This relates to any information that comes to the knowledge of any staff member as a result of exercising a function, e.g. conducting an audit, under these Acts.

Under the NSW *Privacy and Personal Information Protection Act 1998*, the Audit Office is required to manage personal information in accordance with the Information Protection Principles. Under the NSW *Health Records and Information Privacy Act 2002*, the Audit Office is required to manage health information in accordance with the Health Privacy Principles. A data breach involving personal information or health information may be the result of a breach of the Information Protection Principles or the Health Privacy Principles. For further information, refer to the Audit Office's Privacy Management Plan.

7 Definitions

Data breach – A data breach occurs when an incident has caused or has the potential to cause unauthorised access to information collected by the Audit Office (including information collected by the Audit Office from its auditees), such as:

- accidental loss or theft of material on which unencrypted data is stored (e.g. loss of paper record, upload of data to unsecure file sharing platform)
- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- unauthorised disclosure of material or information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the Audit Office website without consent
- unauthorised sharing of information with other internal staff or external individuals
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- successful attempts to gain unauthorised access to Audit Office information or information systems
- data being stored in an improperly secured location that would allow for unauthorised access

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

8. Contact point

Any inquiries concerning the Policy, or its application should be directed to the Audit Office's Privacy Contact Officer (the Executive Manager, Governance (Legal)).

9. Review

This Policy will be reviewed at least every two years 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 – Data breach response checklist

To be completed by the Response Coordinator

Name:		**Role:**	

Short name for breach	[*Insert a short name for the breach – for example 'Department X – payroll data – financial audit'*]

1. Contain the breach	
Measures have been taken to contain the breach. **Note**: See the table in section 3 of this Policy for steps to contain an email that has been sent to the wrong recipient.	[*Insert an overview of the measures taken*]
Note: Preliminary notification should be made as soon as possible and within the first few hours. A subsequent meeting (within 48 hours) can address mitigating actions that have been taken to contain the breach.	☐ Deputy Auditor-General notified Date and time of notification: [*hh:mm, dd mm yy*]
If the breach is via electronic means, the Service Desk has been notified.	☐ Service Desk notified Date and time of notification: [*hh:mm, dd mm yy*] ☐ Service Desk not required to be notified
Notify the Data Breach Response team:	Date and time of notification: [*hh:mm, dd mm yy*] ☐ ☐ ☐
2. Evaluate the associated risks	
What type of data is involved in the breach? Are there indications that the data was accessed by an unauthorised person?	
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?	
Other notes	
Further remedial action identified.	**Recommended remedial actions** / **Completed Y/N** 1. 2. 3.
3. Consider notifying affected individuals/organisations	
What is the risk of harm to the individual/organisation? (refer Appendix B)	
What steps have been taken to date to avoid or remedy any actual or potential harm?	
What is the ability of the individual/organisation to take further steps to avoid or remedy harm?	
Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?	
Is it recommended that affected individuals/organisations be notified?	Y/N
Did the data breach involve a TFN?	Y/N
Any notification has been approved by the Deputy Auditor-General?	Y/N

Have notifications been made?	List individuals/organisations notified: <table><tr><th>Individual/organisation</th><th>Date notified</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table> If a TFN is involved, has the OAIC notified? <table><tr><td>Y/N</td><td>[*If yes, insert date notified*]</td></tr></table> Note any further action arising:
4. Prevent a repeat	
A post-breach review and report to the Deputy Auditor-General/Office Executive on outcomes and recommendations has been prepared. *See template in Appendix C.*	☐ Report provided Date of reporting: [*dd mm yy*]
A copy has been provided to the Chief Information Officer and the Privacy Contact Officer.	☐ Report provided Date of reporting: [*dd mm yy*]
Other follow up actions:	

Appendix B – Guidance for assessing risk of serious harm

The risk of serious harm must be assessed on a case-by-case basis. Each data breach will be different. For the purposes of this Policy, a data breach has been defined as 'an incident that has caused or has the potential to cause unauthorised access to information collected by the Audit Office'. 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, depend only on the type of information involved but there are a range of other considerations that must be made when considering the impact of a data breach. These will include the type of information involved, the extent of the breach, the nature of the breach, and the type of potential harm. This guide lists elements that should be considered when assessing whether a data breach is likely to result in serious harm:

A. Type of information

1. What is the information that is the subject of the data breach?
2. Is the information sensitive or confidential?
3. Is the data breach a breach of privacy (i.e. involving personal information)?
    a) If so, does the breach involve health information?
    b) Can individuals be identified by the information?
    c) Does the information relate to individuals who are vulnerable such that the harm caused by the data breach is potentially greater?
    d) It is also relevant to consider whether more than one type of personal information has been affected by the data breach, as a combination of types of personal information will allow more to be known about the individual(s) affected and increase the risk of serious harm.
4. Is the data breach a breach of sensitive commercial information?
5. Is the data breach a breach of sensitive government information?
6. Is the data breach a breach of sensitive NSW Cabinet information?
7. Is the data of poor quality or able to be misconstrued to the detriment of an individual(s), an organisation or the government?

B. Extent of the breach

8. How long has the information been accessible (the longer the time, the greater the potential for harm)?
9. Was the information encrypted, redacted or otherwise protected? Could the security measures protecting the information be overcome/circumvented?
10. Has, or can, the breach be easily contained?
11. How many people have, or could potentially have, unauthorised access to the information?
12. How many people have been, or are likely to be, affected by the breach?

C. Nature of the breach

13. Who is the known, or likely, recipient of the information or individual(s)/system(s) that have had, or may have, unauthorised access to the information?
14. Was the breach an individual inadvertent mistake, a symptom of a systemic issue or a malicious attack?
15. Does the breach contravene a law or security requirement?
16. Has the data breach resulted in, or has the potential to result in, the alteration of information?
17. Has an operating system or other system been corrupted by the breach?
18. Has the data breach sequestered information so that it is no longer accessible or able to be properly administered?

D. Type of potential harm

19. What sort of harm is likely to arise from the data breach? Some examples include:
    - risk to the physical safety of an individual or individuals
    - risk of identity theft
    - financial loss
    - commercial risk
    - the integrity of an administrative or judicial process
    - damage to reputation – this may be an individual's reputation or an organisation's reputation, but it may also extend to the potential loss of public trust in an agency or government program
    - damage to relationships
    - workplace bullying or marginalisation
    - operational or strategic damage to an organisation
    - risk of further data breaches using the information from the present data breach.

Because of the specific nature of data breaches, no single formula can be provided for determining the likelihood of serious harm as a result of a data breach. Rather, the list above should be used as a way of thinking through all of the potential factors that may contribute to, or ameliorate, serious harm.

The Commonwealth *Privacy Act 1988* makes reference to what a 'reasonable person' might consider to be a risk of serious harm. This may be helpful to officers charged with considering whether there is a risk of serious harm. In guidelines issued by the OAIC (Australian Privacy Principles Guidelines), the following further explanation about reference to a 'reasonable person' is made:

> *What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices. It is the responsibility of an … entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person'; it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'. As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.*

OAIC, APP Guidelines, July 2019.

Those responsible for considering the likely harm of a 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, Corporate Services
- Executive Director, Professional Services
- Chief Information Officer
- Privacy Contact Officer.

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

Appendix C – Template briefing note for the Office Executive

To:	Office Executive	**Agenda #**	[*Meeting agenda #*]
Subject:	Data breach: [ ]	**Date:**	[*Date*]
From	XX – Response Coordinator	**Ref:**	[*HPCM number*]
Sponsor:	[*Committee Member Name and title*]		
Response to:	In response to a data breach where [ ]		

Purpose

The purpose of this brief is to inform the Office Executive of the data breach incident that occurred on [date].

Background information

[*Insert a brief outline of the nature of the data breach*]

Four stages of the Data Breach Management Policy

The response to this incident followed the four stages prescribed in the Data Breach Management Policy:

1. Containment

[*Insert a brief outline of the steps undertaken to contain the data breach*]

2. Evaluate the risks

[*Insert a brief outline of the evaluation of the risks associated with the data breach*]

3. Notifying

[*Insert a brief outline of the decisions concerning notification of individuals/organisations about the data breach*]

4. Prevent

[*Insert a brief outline of the ways the data breach will be prevented in the future*]

Detail of proposed enhancements to existing controls

[*Outline any proposed enhancements to existing controls*]

Detail of proposed additional preventative actions

[*Outline any additional preventative actions proposed*]

Action or recommendation

For the Office Executive to note the response to the data breach.

Appendix D – Template for written notification of data breach

Dear [name]

I am writing to you with important information about a recent data breach involving your personal information / information about your organisation. The Audit Office became aware of this breach on [date]. The breach occurred on or about [date] and occurred as follows [Describe the event, including, as applicable, the following:

- A brief description of what happened.
- Description of the data that was inappropriately accessed, collected, used or disclosed.
- Risk(s) to the individual/organisation caused by the breach.
- Steps the individual/organisation should take to protect themselves from potential harm from the breach.
- A brief description of what the Audit Office is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.]

Please call me with any questions or concerns you may have about the data breach. We take our role in safeguarding your data and using it in an appropriate manner very seriously. Please be assured that we are doing everything we can to rectify the situation.

[In the case of loss of personal information] Please note that under the *Privacy and Personal Information Protection Act 1998* / *Health Records and Information Privacy Act 2002* [select applicable] you are entitled to register a complaint with the NSW Privacy Commissioner with regard to this breach. Further information about registering a complaint can be found on the website of the Information and Privacy Commission NSW.

Should you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me.

Yours sincerely

[Insert applicable name and contact information]