|  |  |
| --- | --- |
| Policy No: 3.16 | Policy Name: Notifiable Data Breaches |

|  |  |
| --- | --- |
| Applies to:  | Version:  |
| Specific responsibility:  | Date Approved: |
|  | Review Date: |

# Purpose

The purpose of this policy is to respond to the Privacy Amendment (Notifiable Data Breaches) Act 2017 and to protect the privacy rights of clients accessing [Service Name].

This policy applies to all [Service Name] staff members, students, volunteers and Board members.

# Policy statement

As an organisation regulated under the Australian Privacy Act 1998 (Cwlth), [Service Name] operates within the regulations of the NDB scheme.

The NDB scheme strengthens protections for personal information and allows individuals to take steps to protect their information when a breach of data, or a suspected breach, in relation to that person is made by an organisation that holds such data. The NDB scheme requires organisations to undertake the following steps:

* assess when there has been a data breach
* notify the affected individual(s)
* notify the office of the Australian Information Commission (OAIC) when a data breach is likely to result in serious harm to the individual(s) whose personal information is involved in the breach.

[Service Name]’s commitment to the NDB scheme is demonstrated by its implementing of timely assessments and response processes when a data breach has occurred.

# References

Office of the Australian Information Commissioner

**Federal Circuit Court of Australia (Consequential Amendments) Act 2013**

Privacy Amendment (Enhancing Privacy Protection) Act 2012

Health Records and Information Privacy Act 2002 (NSW)

Privacy Act 1988

# Definitions

A **data breach** occurs when personal information is lost or subjected to unauthorised access or disclosure.

The notifiable data breaches (NDB) scheme only applies to data breaches involving personal information that is likely to result in serious harm to any individual affected. These are considered eligible data breaches.

Examples of a data breach include the following incidents:

* A client’s personal information is lost or stolen.
* A database containing personal information is hacked.
* Personal information is mistakenly provided to the wrong person.

# Procedure

## Eligible data breaches

A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

If a data breach is likely to result in serious harm, then an objective assessment is to be completed from the perspective of a reasonable person.

A reasonable person denotes someone in [Service Name] who is properly informed about the matter, based on information that is immediately available or following reasonable inquiries about the data breach.

If [Service Name] acts quickly to remediate a data breach, and the data breach is not likely to result in serious harm due to this action, then there is no requirement to notify any individual or the Commissioner.

## Assessing for an eligible data breach

An assessment of an eligible data breach must be conducted within 30 calendar days of the initial breach incident.

The following three criteria must be met to determine an eligible data breach:

1. **Unauthorised access** – [Service Name] has disclosed personal information that is unauthorised, or the information has been accessed inadvertently. Examples of unauthorised access include
* a staff member browsing sensitive client records without any legitimate purpose
* a computer network being hacked, resulting in personal information being accessed without authority
* a staff member accidentally publishing a confidential data file containing the personal information
* client information that is lost, either in the workplace due to an unsecured computer or outside the workplace due to reasons such as transporting a client’s file.
1. **Likelihood of serious harm** - the second step in deciding whether an eligible data breach has occurred involves deciding from the perspective of a reasonable person whether the data breach would likely result in serious harm to an individual whose personal information was part of the data breach.

The phrase ‘likely to result’ means that the risk of serious harm to an individual is more probable than not (rather than possible).

Serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm, such as:

* identity theft, which can affect a person’s finances and credit report
* financial loss through fraud
* a likely risk of physical harm, such as by an abusive ex-partner
* serious psychological harm
* serious harm to an individual’s reputation.

[Service Name] will assess the risk of serious harm holistically. The following should be considered when assessing the likelihood of serious harm:

* the type of information
* the sensitivity of the information
* whether the information is protected by one or more security measures
* the likelihood that any of these security measures could be overcome (if the information is protected by one or more security measures)
* the persons who have obtained, or who could obtain, the information
* the likelihood that harm will occur to any of the individuals to whom the information relates
* the nature of the harm.
1. **Preventing serious harm with remedial action—'**remedial action’ signifies taking steps to prevent the unauthorised access or disclosure of personal information.

If the remedial action prevents the likelihood of serious harm to individual(s), then notification of a potential data breach is not required, as the breach has been prevented.

Examples of remedial action include

* contacting external agencies and requesting information to be deleted if personal information is accidentally sent
* applying technology to delete content if a smartphone device is lost.
1. **Response plan**—The flowchart below can be used when responding to data breaches. The diagram is sourced from the OAIC Guide to Managing Data Breaches in accordance with the Privacy Act 1988 (Cwlth).



The [Manager] will be responsible for managing any data breach incidents. The [Manager] is responsible for assessing, investigating, notifying and reviewing data breaches.

The following stages in Table 1 are required when responding to a potential data breach.

Table 1: Actions in Response to Data Breaches.

|  |  |
| --- | --- |
| **STAGE**  | **ACTION** |
| IDENTIFY  | When staff have reason to believe that there has been a data breach, they should inform their Manager immediately. Details such as when and how the breach was discovered, and by who, should be recorded in the Data Breach Incident Reporting form. |
| CONTAIN  | As soon as a breach or suspected breach has been identified, any steps to contain or limit the potential harm should be taken. This may include shutting down a system that has been breached or recovering any records.The staff member who discovers the breach, in consultation with his or her manager, will complete a preliminary assessment of the breach and take any immediate action to contain the breach, if possible.  |
| ASSESS | The three-stage process below is suggested by the OAIC: **Initiate**—decide whether an assessment is necessary and identify which person or group will be responsible for performing it. **Investigate—**quickly gather relevant information about the suspected breach, including what personal information is affected, who may have had access to the information and the likely effects.**Evaluate**—make a decision based on the investigation about whether the identified breach is an eligible data breach. |
|  | To evaluate whether a known data breach is notifiable, consider the following three questions:* Has there been unauthorised access, unauthorised disclosure, accidental loss or theft of personal information that the organisation holds?
* Is it *likely* that this may result in *serious* harm to individual(s) whose data has been breached?
* Does the likelihood of serious harm remain despite taking available remedial action?
 |
|  | If answers to the above three questions are yes, then the breach classifies as an eligible data breach and organisations are required to notify the OAIC and any affected individuals.  |
| REMEDIAL ACTION  | Remedial action can be taken at any point throughout the data breach response process. The process of any remedial action should be documented, ensuring that any rationale and reasoning for why a certain conclusion has been made is documented. If the risk of harm is reduced so that it is unlikely to occur, or it is non-serious, after the remedial action has been taken, then there is no requirement to notify. |
| NOTIFY | Once a breach has been assessed as eligible, the OAIC should be notified as soon as practicable. Notification must include the following information as a minimum:* the organisation’s name and contact details
* a description of the data breach
* the type of information involved in the breach
* advice and recommendations for individuals to take in response.

The [Manager] is responsible for notifying and liaising with the OAIC for data breaches that have been assessed as eligible for the purposes of the NDB scheme. The [Manager] uses the OAIC’s Notifiable Data Breach Form<https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB>*.*  |
|  | The way that notification to individuals occurs will depend on the context and nature of the breach, as well as on the relationship of the affected individuals to the organisation. Notification should occur as soon as practicable after completing the notification statement for the OAIC. |
| RECORD AND REVIEW  | [Service Name] will keep a data breach log to record all instances of data breaches or suspected breaches; it will also document assessments of the breach and any changes that were made due to a breach. All staff should be made aware of the log, and the Executive Director will be responsible for ensuring that all breaches or suspected breaches are recorded accurately in the log.  |
|  | Regardless if the breach or suspected breach was notifiable or not, a review should be conducted of the processes relating to the breach, so that protections in the future can be strengthened. Depending on the type and seriousness of the breach, this may include:* conducting a full investigation into how the breach occurred
* implementing measures to ensure that it does not re-occur, which are documented in a prevention plan
* reviewing security systems and cybersecurity
* reviewing relevant policies and procedures
* providing additional staff training in regard to privacy and data breach responses.
 |

## Issues to consider to minimise the impact of a data breach

There are a number of issues that [Service name] might consider as they develop systems to minimise the impact of a data breach. These include:

Adequate insurance protection

* undertake a review of insurances held to ensure they provide adequate protection in the event that a ransomware attack is launched against the service.
* Initiate a discussion with an insurance broker to explore insurance cover available

Time impact regarding management of a data breach

* Prepare for commitment of significant hours as a data breach is explored and managed in conjunction with the Privacy Commission, clients and other key contacts

Manage and support those who are impacted by the data breach

* Establish a key contact person who will be available to advise people who are impacted by the data breach about what has happened, provide guidance on steps they need to take to secure their information and co-ordinate the communication strategy development

Develop a communication strategy

* Establish information on [Service name] website to identify that a data breach has occurred and to provide direction for those who might be affected by this
* Create and distribute a letter from [Service name] to all who might be affected by the data breach outlining what has happened and provide guidance on steps they need to take to secure their information

Review and update [Service name] risk management plan.

# Related documents

Communication Policy

Privacy and Confidentiality Policy

Staff Induction Policy

# Review

|  |
| --- |
| **Reviewing and approving this policy** |
| Frequency | Person responsible | Approval |
| [How often will this policy be reviewed] | [Position of person responsible for reviewing policy] | [position of person/group who approves this policy] |

|  |
| --- |
| **Policy review and version tracking** |
| Review | Date approved | Approved by | Next review date |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |