**[Company Name]**

**Data Breach Response Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Description of Change** | **Approval** | **Date of Issue** |
| 1.0 |  |  |  |
|  |  |  |  |

# Data Breach Response Plan

## Background

### A data breach occurs when when personal information that an entity holds is subject to **unauthorised access or disclosure or is lost**[[1]](#footnote-2).

### The consequences of a data breach can result in serious harm to any of the individuals to whom the information relates, may damage the reputation of the [Company / organisation name] and leave the [Company / organisation name] in breach of its obligations under the *Privacy Act 1988* (Cth)[[2]](#footnote-3).

### [Company / organisation name] is responsible for ensuring that all reasonable steps are taken to handle personal information in accordance with the Australian Privacy Protection Principles[[3]](#footnote-4). This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification and disclosure.

### The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB Act) established the Notifiable Data Breach (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. Where it is determined there is an eligible data breach, the Office of the Australian Information Commissioner (OAIC) must also be notified.

### Accordingly, [Company / organisation name] must be prepared to act quickly in the event of a data breach (or suspected breach) and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

### Adherence to this procedure will ensure the [Company / organisation name] can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person/s affected.

### This plan has been informed by:

* The OAIC’s *Guide to developing a data breach response plan[[4]](#footnote-5)*
* The OAIC’s *Data breach notification guide: a guide to handling personal information security breaches[[5]](#footnote-6)*
* The NDB Act
* The Privacy Act and Australian Privacy Principles (Schedule 1 of the Act)

### [Provide additional context, as required.]

## Objectives

### This data breach response plan sets out the roles, responsibilities and processes in the event of a data breach or suspected data breach.

## Report Data Breaches and Suspected Data Breaches

### Any staff who suspect or become aware of a data breach must immediately alert their [supervisor / manager] and then complete a Data Breach Report (Annex A, Section 1) and forward the completed report to the Privacy Officer, copied to their [supervisor / manager].

### Information to be included in the report (if known) should include:

* when the breach occurred (time and date);
* description of the breach (type of Personal Information involved);
* cause of the breach (if known), or how it was discovered;
* which systems/s, if any, are affected;
* which part of the business is involved; and,
* whether corrective action has occurred to contain or remediate the breach (or suspected breach).

### Note, a full forensic investigation may be required to provide detailed answers on the nature, extent and impact of the breach. [Insert additional details here on Cyber Insurance policy, name of Incident Response retainer company and how to activate response capability or name and details of trusted third-party provider, Legal Counsel, etc.]

## Informing the Data Breach Response Team [Or insert other name for this team / response]

### Following receipt of a Data Breach Report, or otherwise being notified of a data breach or suspected data breach, the Privacy Officer must inform the Data Breach Response Team, the CEO and [others].

### The Data Breach Response Team consists of the following:

* [Title / Position (Chair)];
* [Title / Position]; and,
* Any other person considered necessary by the Chair of the Data Breach Response Team.

## Assess and Determine the Potential Impact

### Once notified, the Data Breach Response Team will consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgment as to its severity (Annex A, Section 2).

### Criteria for determining whether a privacy data breach has occurred is as follows:

### Is Personal Information involved?

### Is the Personal Information of a sensitive nature?

### Has there been unauthorised access to Personal Information, or unauthorised disclosure of Personal Information in circumstances where access to the information is likely to occur?

### For the purposes of this assessment the following terms are defined in the [Company / Organisation name’s] Privacy Policy [(reference or link)]: Personal Information, sensitive information, unauthorised access, unauthorised disclosure and loss.

### Criteria for determining severity is as follows:

### The type and extent of Personal Information involved;

### Whether multiple individuals have been affected;

### Whether information is protected by any security measures (password protection or encryption);

### The person or kinds of people who now have access;

### Whether there is (or could be) a real risk of serious harm to the affected individuals;

### Whether there could be media or stakeholder attention as a result of the breach or suspected breach; and,

### With respect to (e) above, serious harm could include physical, physiological, emotional, economic/financial harm to reputation and is defined in section 26WG of the NDB Act.

## Responding to a Data Breach

### Following notification of the breach (or suspected breach), the Data Breach Response Team will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Instructions will be issued regarding how the data breach should be managed, depending on the nature and severity of the breach.

### There is no single method of responding to a data breach and each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate action.

### The following steps may be undertaken, as directed by the Data Breach Response Team:

### Immediately contain the breach;

### Ensure corrective action is taken;

### Corrective action may include retrieval or recovery of the Personal Information, ceasing unauthorised access, shutting down or isolating the affected system

### Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach;

### Call upon the expertise of, or consult with, relevant staff;

### Assess whether serious harm is likely; and,

### Make a recommendation to the [Chair / CEO] whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals; and,

### Consider developing a communication or media strategy including the timing, content and method of any announcements.

## Finalisation of the Report and Approval

### The Privacy Office must complete a final assessment and submit the Data Breach Report (within 48 hours of notification) to [Chair / CEO]. The report must contain the following:

### Description of the breach or suspected breach

### Action taken

### Outcome of action

### Processes implemented to prevent a repeat of the situation

### Recommendation that no further action is necessary, or otherwise

### The Data Breach Response Team (usually the [Chair / CEO]) will sign-off that no further action is required.

## Notification of a Data Breach (Affected Individuals)

### In the event of a data breach, including a data breach that is not a notifiable data breach, consideration should be given by the Privacy Officer, Data Breach Response Team and the CEO to notify affected individuals and stakeholder organisations.

### Consideration should also be given to consulting expert third parties, including but not limited to experienced data breach legal counsel and crisis communications specialists, **before** notifying persons potentially affected by a data breach.

### [In addition, consideration should always be given to voluntarily notifying a data breach to the Office of the Australian Information Commissioner, even if it is *not* an eligible data breach under the Data Breach Notification scheme in the Privacy Act.]

## Notifiying the OAIC

### Where it is determined there is an eligible notifiable data breach, the OAIC should be notified ([Notifiable Data Breach Form](https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion)). This form is used to inform the Australian Information Commissioner of an eligible data breach where required by the *Privacy Act 1988*.

1. The Data Breach Response Team will provide guidance on completion of this form to the Privacy Officer.
2. Consideration should also be given to consulting expert third parties, including but not limited to experienced data breach legal counsel and crisis communications before, **before** notifying the OAIC.

### Part one is the statement about a data breach, as required by section 26WK of the Privacy Act. Part two of the form is optional, however the OAIC encourages voluntary provision of additional information.

1. An example form is provided by the OAIC [here](https://www.oaic.gov.au/__data/assets/pdf_file/0008/2240/oaic-ndb-form-for-training-purposes-only.pdf).

### Part one includes organisation details, description of the eligible data breach, information involved (personal, financial, sensitive) and recommended steps. The section about ‘other entities affected’ is optional.

### Part two is for additional information, including breach details, date of identification, primary cause, numerb of individuals affected, description of action including remedial steps, details of the notification campaign and other authorities notified (law enforcement, regulatory bodies, etc).

## Review of the Incident

### The Data Breach Response Team is responsible for reviewing the incident (Annex A, Section 3). It is important to capture:

### Lessons learnt and remedial action to reduce the likelihood of recurrence – this may involve a review of policies, processes and refresher training.

### Relevant work areas responsible for implementation of any changes as a result of lessons learnt and reviews.

### The Privacy Officer must provide a final report on the incident to the Data Breach Response Team, including a review of the incident.

# Document Control

## Review

### This Policy will be formally reviewed annually, as a minimum, or if changes are required.

### The [Title / Position] is the owner of this document and is responsible for ensuring it is reviewed. [Title / Position] is the document approver.

# ANNEX A: DATA BREACH REPORT

**Section 1: Report data breach or suspected data breach**

Staff are required to alert [supervisor / manager] immediately following identification of a data breach, or a suspected data breach and complete Section 1 of this report.

|  |  |
| --- | --- |
| **Date of breach:** | Click or tap to enter a date. |
| **Time of breach:** | Click or tap here to enter text. |
| **Description of breach:** | [describe the type of personal information involved eg contact details, date of birth] |
| **Cause of breach:** | [if unknown, explain how the data breach was discovered] |
| **Which system(s), if any, are affected?** | Click or tap here to enter text. |
| **Which section is involved?** | Click or tap here to enter text. |
| **Has corrective action occurred to remedy or ameliorate the breach or suspected breach? If so, what?** | Click or tap here to enter text. |
| **Alert made by:** | [Name of Company Staff] |
| **Date:** | Click or tap to enter a date. |

**Section 2: Assess and determine potential impact**

The Data Breach Response Team must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

|  |
| --- |
| *Alert received by:* |
| **Name:** | Name |
| **Date:** | Click or tap to enter a date. |
| *Criteria for determining whether a privacy data breach has occurred* |
| **Is personal information\* involved?** | Yes [ ]  No [ ]   |
| **Is the personal information of a sensitive\* nature?** | Yes [ ]  No [ ]  |
| **Has there been unauthorised access\* to personal information, or disclosure\* of personal information, or loss\* of personal information in circumstances where access to the information is likely to occur?** | Yes [ ]  No [ ]   |
| *Criteria for determining severity* |
| **Describe the type and extent of personal information involved:** | Click or tap here to enter text. |
| **Have multiple individuals have been affected?**  | Yes [ ]  No [ ]  If yes, provide further details:  |
| **Confirm whether the information is protected by any security measures:** | Yes [ ]  No [ ]  If yes, provide further details: |
| **Provide details on the person or kinds of people who now have access:** | Click or tap here to enter text. |
| **Determine whether there is (or could be) a real risk of serious harm\* to the affected individuals:** | Click or tap here to enter text. |
| **Determine whether there could be media or stakeholder attention as a result of the breach or suspected breach:** | Click or tap here to enter text. |

**Section 3: Data breach review**

|  |  |
| --- | --- |
| **Description of breach:** | Click or tap here to enter text. |
| **Action taken:** | Click or tap here to enter text. |
| **Outcome of Action** | Click or tap here to enter text. |
| **Processes implemented to prevent a repeat of the situation** | Click or tap here to enter text. |
| **Any other information of relevance** | Click or tap here to enter text. |
| **Recommendation to the Privacy Officer** | i.e no further action is necessary |
| *Report submitted by:* | [Name of Company Personnel] |
| **Date:** | Click or tap to enter a date. |
| *Privacy Officers’ determination that no further action is necessary* | Yes [ ]  No [ ]   |
| **Signed:** | [signature of Privacy Officer] |
| **Date:** | Click or tap to enter a date. |

1. https://www.oaic.gov.au/privacy/notifiable-data-breaches [↑](#footnote-ref-2)
2. https://www.legislation.gov.au/Series/C2004A03712 [↑](#footnote-ref-3)
3. https://www.oaic.gov.au/privacy/australian-privacy-principles [↑](#footnote-ref-4)
4. https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-2-preparing-a-data-breach-response-plan [↑](#footnote-ref-5)
5. https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response [↑](#footnote-ref-6)