[Insert organisation name/logo]

[INSERT ORGANISATION NAME] DATA BEACH RESPONSE PLAN

The passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* established a Notifiable Data Breaches (NDB) scheme in Australia. Commencing from 22 February 2018, the NDB scheme requires organisations covered by the Australian *Privacy Act 1988* (the Act) to notify any individuals likely to be at risk of serious harm by a data breach. The notice must include recommendations about the steps individuals should take in response to the data breach, including notifying the Australian Information Commissioner.

## What is a data breach?

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Personal information is information or an opinion about an identified or reasonably identifiable individual. Data breaches may include (but are not limited to) unauthorised access by a third party, information accidentally being uploaded to a public website or a laptop or USB drive containing personal information being lost or stolen and can be caused by or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies or organisations.

## Which data breaches are notifiable?

Not all data breaches require notification. The NDB scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates. The purpose of this plan is to enable that assessment to be undertaken and for [insert organisation name] to meet its reporting obligations.

## Data breach plan

This data breach response plan outlines definitions, sets out procedures and clear lines of authority for [insert organisation name] staff in the event that [insert organisation name] experiences a data breach, or suspects that a data breach has occurred.

This response plan is intended to enable [insert organisation name] to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist [insert organisation name] to respond to a data breach.

# Assessing suspected data breaches

If any [insert organisation name] staff member suspects or becomes aware of a data breach, this plan is activated and must be followed. The plan requires a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm. The following chart outlines the staff roles involved in assessing a data breach.

**ALERT NADA DATA BREACH RESPONSE TEAM COORDINATOR [insert responsible person, e.g. Admin Manager]**

Coordinator convenes Response Team

**WHAT SHOULD THE [insert responsible person, e.g. Clinical Director] DO?**

* Determine whether a data breach has or may have occurred.
* Determine whether the data breach is serious enough to escalate to the Data Breach Response Team.
* If so, immediately escalate to the Data Breach Response Team.

**Data Systems**

**Primary Contact**

**Secondary Contact**

**ICT**

**Primary Contact**

**Secondary Contact**

**Business Systems**

**Primary Contact**

**Secondary Contact**

**Communications**

**Primary Contact**

**Secondary Contact**

**WHAT SHOULD THE [insert organisation name] STAFF MEMBER DO?**

* Immediately notify the [insert responsible officer, e.g. Clinical Director] of the suspected data breach.
* Record and advise the [insert responsible officer, e.g. Clinical Director] of the time and date the suspected data breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

**[insert organisation name] EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED**

Discovered by [insert organisation name] staff member, or [insert organisation name] otherwise alerted

## When should the [insert responsible person, e.g. Clinical Director] escalate a data breach to the [insert organisation name] Data Breach Response Team?

**[insert responsible person, e.g. Clinical Director] to use discretion in deciding whether to escalate to the Response Team.**

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (**Response Team**).

An example is, a [insert organisation name] officer may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the officer can contact the recipient and the recipient agrees to delete the email, it may be that there is no need to escalate the issue to the Response Team as there is no risk of serious harm to the individual whose personal information has been inadvertently disclosed.

The [insert responsible person, e.g. Clinical Director] should use their discretion in determining whether a data breach or suspected data breach requires escalation to the Response Team. In making that determination, the [insert responsible person, e.g. Clinical Director] should consider the following questions:

* Are multiple individuals affected by the breach or suspected breach?
* Is there (or may there be) a real risk of serious harm to the affected individual(s)?
* Does the breach or suspected breach indicate a systemic problem in [insert organisation name] processes or procedures?
* Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is ‘yes’, then it may be appropriate for the [insert responsible person, e.g. Clinical Director] to notify the Response Team.

**[insert responsible person, e.g. Clinical Director] to inform the Response Team Coordinator of minor breaches.**

If the [insert responsible person, e.g. Clinical Director] decides not to escalate a minor data breach or suspected data breach to the Response Team for further action, the [insert responsible person, e.g. Clinical Director] should:

* **send a brief email to the Response Team Coordinator** [insert responsible person, e.g. Admin Manager] that contains the following information:
  + description of the breach or suspected breach
  + action taken by the [insert responsible person, e.g. Clinical Director] or [insert organisation name] officer to address the breach or suspected breach
  + the outcome of that action, and
  + the [insert responsible person, e.g. Clinical Director]’s view that no further action is required
* **save a copy of that email in the following container:**
  + Data Breach Response – reports and investigation of data breaches within [insert organisation name]

# [insert organisation name] Data Breach Response Team

## Response Team membership

The purpose of having a Response Team is to ensure that the relevant staff, roles and responsibilities are identified and documented before the data breach happens. Different skill sets and staff may be needed to respond to one breach compared to another. The [insert organisation name] Response Team are made up of the following staff, including their roles, and has the authority to take the necessary steps in the event of a breach without the need to seek permissions particularly in time critical scenarios.

|  |  |  |
| --- | --- | --- |
| **Team Member** | **Expertise** | **Role** |
| [insert staff name] | [insert staff role in response team, e.g. Team Leader, Coordinator, etc.] | [insert description of responsibilities attributed to role] |
| [insert staff name] | [insert staff role in response team, e.g. Team Leader, Coordinator, etc.] | [insert description of responsibilities attributed to role] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Process

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected data breach.

* **STEP 1: Contain the breach and do a preliminary assessment**
* **STEP 2: Evaluate the risks associated with the breach**
* **STEP 3: Notification**
* **STEP 4: Prevent future breaches**

The Response Team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. Refer to the detailed checklist at the end of this plan.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

In reconsidering NADA processes and procedures to reduce the risk of future breaches (Step 4), the Response Team should also refer to [insert organisation name]’s [insert relevant policy, e.g Information and Communications Technology Policy, Privacy and Confidentiality Policy, etc.]. This/these policy/ies outline the security and processes in place that as a result of a data breach should be reviewed and actions considered that may be appropriate to help prevent future breaches following an investigation.

The checklist at the end of this plan is intended to guide the Response Team in the event of a data breach and alert the Response Team to a range of considerations when responding to a data breach.

## Evaluating a serious risk of harm to an individual

In evaluating whether there is a serious risk of harm to an individual whose information is the subject of a data breach, the Response Team must consider:

* what type of personal information is involved (and in particular, whether it is sensitive information);
* whether there are any protections that would prevent the party who receives (or may have received) the personal information from using it (for example, if it is encrypted);
* the nature of the harm that could arise from the breach, for example whether an individual was reasonably likely to suffer:
  + identity theft;
  + financial loss;
  + a threat to their physical safety;
  + a threat to their emotional wellbeing;
  + loss of business or employment opportunities;
  + humiliation, damage to reputation or relationships; or
  + workplace or social bullying or marginalisation;
* what steps have been taken to remedy the breach (and how certain [insert organisation name] is that they are effective).

## Notifying the Office of the Australian Information Commissioner (OAIC)

In the event that the Response Team decides there has been a data breach and there is a real risk of serious harm to affected individuals (Step 3) the Response Team must prepare a statement that includes:

* [insert organisation name]’s contact details;
* a description of the data breach;
* the kind of information concerned; and
* recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

The statement must be submitted to OAIC via email to [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au) as soon as reasonably practical.

## Notifying the individuals affected

As soon as reasonably practical after [insert organisation name] has submitted the statement to the OAIC, [insert organisation name] must:

* if practical, take reasonable steps to notify the contents of the statement to each of the individuals to whom the information relates; or
* if practical, take reasonable steps to notify contents of the statement to each of the individuals who are at risk from the eligible data breach.

If it is not practical to undertake either of the above, the Response Team must ensure a copy of the statement is published on [insert organisation name]’s website and reasonable steps are taken to publicise the contents of the statement (for example, by notifying its members).

## Records Management

Documents created by the Response Team should be saved in the following container:

* Data Breach Response – reports and investigation of data breaches within [insert organisation name]

|  |  |  |
| --- | --- | --- |
| **STEP 1**  **Contain the breach and make a preliminary assessment** | **☐** | Convene a meeting of the data breach Response Team. |
| **☐** | Immediately contain breach:   * IT to implement the ICT Incident response plan if necessary * Building security to be alerted if necessary |
| **☐** | Inform the [insert responsible person/s, e.g. Executive team], provide ongoing updates on key developments. |
| **☐** | Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing [insert organisation name] to take appropriate corrective action. |
| **☐** | Consider developing a communications or media strategy to manage public expectations or media interest. |
|  |  |  |
|  | **☐** | Conduct initial investigation, and collect information about the breach promptly, including:   * the date, time, duration and location of the breach * the type of personal information involved in the breach * how the breach was discovered and by whom * the cause and extent of the breach * a list of the affected individuals, or possible affected individuals * the risk of serious harm to the affected individuals * the risk of other harms |
| **☐** | Determine whether the content of the information is important. |
| **☐** | Establish the cause and extent of the breach. |
| **☐** | Assess priorities and risk based on what is known. |
| **☐** | Keep appropriate records of the suspected breach and actions of the Response Team, including the steps taken to rectify the situation and the decisions made. |
| **STEP 2**  **Evaluate the risks for individuals associated with the breach** |  |  |
| **STEP 3**  **Consider breach notification** | **☐** | Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage. |
| **☐** | Determine whether to notify affected individuals – is there a *real risk of serious harm to the affected individuals?* |
| **☐** | Consider whether others need to be notified, including police, Australian Privacy Commissioner, or other agencies or organisations affected by the breach, or where [insert organisation name] is contractually required, or required under the terms of an MOU to notify specific parties. |
|  |  |  |
| **STEP 4**  **Review the incident and take action to prevent future breaches** | **☐** | Fully investigate the cause of the breach. |
| **☐** | Report to [insert responsible person/s, e.g. Executive team] on outcomes and recommendations:   * update security and response plan if necessary * make appropriate changes to policies and procedures if necessary * revise staff training practices if necessary * consider the option of an audit to ensure necessary outcomes are affected |