**[INSERT ORGANISATION NAME] Data breach incident response plan**

**[Note: this is a template on which the actual plan tailored to the needs of the organisation should be developed]**

Contents

[1. Purpose of this document 1](#_Toc519497946)

[2. Data breach notification process 1](#_Toc519497947)

[3. Data breach notification response 2](#_Toc519497948)

[4. Escalation to the DBIRT 3](#_Toc519497949)

[5. Notifiable data breach response 4](#_Toc519497950)

[6. Related documents 4](#_Toc519497951)

[7. Testing this plan 4](#_Toc519497952)

[8. Records management 4](#_Toc519497953)

[9. Reporting 4](#_Toc519497954)

# Purpose of this document

This data breach incident response plan (response plan) sets out procedures and clear lines of authority for [INSERT ORGANISATION NAME] staff in the event that the [INSERT ORGANISATION NAME] experiences a data breach or suspects that a data breach has occurred.

This response plan is intended to enable the [INSERT ORGANISATION NAME] to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the POPI Act (POPIA) requirements in terms of security compromise management.

A data breach covered by the POPIA or other relevant national legislation occurs when personal information is accidentally or unlawfully destroyed, lost or subjected to unauthorised access or disclosure. For more information see Section 22 of POPIA.

The plan 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.

# Data breach notification process

A data breach suspected by a staff member or other stakeholder (e.g. contractor, customer or supplier) may be reported to [insert contact details] supplying the following details:

* time and date the suspected breach was discovered,
* type of personal data involved,
* cause and extent of the breach if known, and
* context of the affected data and the breach.

# Data breach notification response

The Information Officer (IO) will:

* Determine whether a data breach has or may have occurred.
* Determine whether the data breach is serious enough to escalate to the Data Breach Incident Response Team (DBIRT) (some breaches may be able to be dealt with at the IO level)
* Determine whether this is a notifiable breach to affected individuals and supervisory authorities in terms of the relevant legislation.

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

Step 1: Contain the breach

* Notify the IO, who may convene the DBIRT.
* IO will take steps to immediately contain breach:
  + IT to implement the ICT Incident Response Plan if necessary.
  + Building security to be alerted if necessary.
  + Consider whether other parties needs to be advised.
* Consider whether IO or DBIRT needs additional expertise assistance (e.g. data forensics specialists)
* IO will inform the [INSERT ORGANISATION NAME] Executive, as soon as possible; provide ongoing updates on key developments.
* IO will ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the [INSERT ORGANISATION NAME] to take appropriate corrective action.
* IO will consider a communications or media strategy to manage public expectations and media interest.

Step 2: Assess the risks for individuals associated with the breach

* Conduct initial investigation, and collect information about the breach promptly, including:
  + the date, time, duration, and location of the breach
  + the type of personal data 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 context of the data is important.
* Establish the cause and extent of the breach.
* Assess priorities and risks 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 3: Consider breach notification

* Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage. This is based on the recommendations of the IO
* Determine whether and how to notify affected individuals. Does the breach trigger the requirements of the POPIA – is the breach likely to result in serious harm to any of the individuals to whom the information relates and the [INSERT ORGANISATION NAME] has not been able to prevent the likely risk of serious harm through remedial action. In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals. If the POPIA notification is triggered – a formal notification to the supervisory authority through their mechanism should be completed and recorder in the IO incident record.
* Consider whether others should be notified, including the police/law enforcement, or other agencies or organisations affected by the breach or can assist in containing the breach or assisting individuals affected by breach, or where the [INSERT ORGANISATION NAME] is contractually required or required under the terms of a contract, code or practice or similar obligation to notify specific parties.

Step 4: Review the incident and take action to prevent future breaches

* Fully investigate the cause of the breach.
* Implement a strategy to identify and address any weaknesses in data processing that contributed to the breach
* Conduct a post-breach review and report to [INSERT ORGANISATION NAME] Executive 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 effected

# Escalation to the DBIRT

The IO will use their discretion in deciding whether to escalate to the DBIRT. Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Incident Response Team (DBIRT). In making that determination, the IO will 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 any of 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 the IO will convene a meeting (face-to-face or virtual) of a quorum of the Data Breach Incident Response Team (DBIRT).

For example, an [INSERT ORGANISATION NAME] staff member may, as a result of human error, send an email containing personal data to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the officer can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the response team or initiating the notification process.

DBIRT team members for [INSERT ORGANISATION NAME] are shown in the following table. A quorum represents 75% [or choose another %] or more of the total DBIRT team or their nominated alternate:

[complete following table]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of DBIRT team member** | **Job title** | **Alternate representative** | **Job title** | **DBIRT role** |
| Name | Information Officer | Name | Title | Role |
| Name | Title | Name | Title | Role |
| Name | Title | Name | Title | Role |
| Name | Title | Name | Title | Role |
| Name | Title | Name | Title | Role |
| Name | Title | Name | Title | Role |
| Name | Title | Name | Title | Role |

# Notifiable data breach response

The checklist below sets out the steps that the IO will take with approval of the DBIRT in the event of a notifiable data breach.

* Initiate identification and notification to impacted individuals
* Initiate notification to the relevant supervisory authority
* Prepare a corporate communication on the nature and impact of the data breach for use with external stakeholders (other than supervisory authority and impacted individuals e.g. to the media)

# Related documents

The IO and DBIRT will consider the following documents where applicable:

[Insert related document names e.g. business continuity or IT disaster recovery plan]

# Testing this plan

Members of the DBIRT should test this plan with a hypothetical data breach at least annually to ensure that it is effective. As with the post-breach review following an actual data breach, the response team must report to the [INSERT ORGANISATION NAME] IO on the outcome of the test and make any recommendations for improving the plan.

# Records management

Documents created by the IO and DBIRT, including post-breach and testing reviews, should be saved in a manner approved by the IO:

# Reporting

The IO will ensure reporting of all reported incidents is included in the periodic IO reports. The report of incidents will include the following details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Date of report** | **Incident reference number** | **Incident brief description** | **Whether incident was a breach in terms of the legislation**  **(Y/N)** | **# of data subjects impacted** | **Data subjects notified**  **(Y/N)** | **Supervisory authority notified (Y/N)** | **Summary of response actions taken** |
|  |  |  |  |  |  |  |  |

**Source acknowledgement:** This plan is based on an original idea from the [www.oaic.gov.au](http://www.oaic.gov.au) and has been amended for use in complying with POPIA.