Data breach response plan
Contents

Data breach response plan 3
Data breach response process 3
Data breach response team — members 4
When should a data breach be escalated to the OAIC Data Breach Response Team? 4
OAIC Data Breach Response Process 5
OAIC’s Data Breach Response Check List 7
Responding to a data breach 9
Data breach response plan

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

A data breach covered by the NDB scheme occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by the OAIC. Data breaches can be caused 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 and entities.

This response plan is intended to enable the OAIC to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the notifiable data breaches (NDB) scheme that commenced on 22 February 2018. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

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 the OAIC to respond to a data breach.

Data breach response process

1 A data breach suspected by a member of the Executive or a Director may be reported directly to the Chief Privacy Officer.

---

1. **OAIC EXPERIENCES DATA BREACH/DATA BREACH SUSPECTED**
   - Discovered by OAIC staff member, contractor or OAIC otherwise alerted

2. **What should the OAIC staff member or contractor do?**
   - Immediately notify your Director EL2 of the suspected data breach.¹
   - Record and advise your Director of the time and date the suspected 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.

3. **What should the Director EL2 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 (some breaches may be able to be dealt with at the Director level).
   - If so, immediately notify the Chief Privacy Officer.

4. **ALERT CHIEF PRIVACY OFFICER — [names redacted]**
   - Chief Privacy Officer convenes data breach response core team
Data breach response team — members

Chief Privacy Officer
[Names redacted]

SCaC Team
Primary contacts
[Names redacted]
Secondary contact
[Names redacted]

DR Branch
Primary contact
[Names redacted]
Secondary contact
[Names redacted]

ICT
Primary contact
[Names redacted]
Secondary contact
[Names redacted]

RS Branch
Primary contact
[Names redacted]
Secondary contact
[Names redacted]

When should a data breach be escalated to the OAIC Data Breach Response Team?

Directors 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).

For example, an OAIC 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 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.

Directors should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, Directors 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 any of the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in OAIC 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 Director should attempt immediate verbal contact with the Chief Privacy Officer, or if this is not possible, another primary response team member.
The checklist below sets out the steps that the response team will take in the event of a serious data breach.

**Directors should inform the Chief Privacy Officer of minor breaches**

If a Director decides not to escalate a minor data breach or suspected data breach to the response team for further action, the Director should:

- send a brief email to the Chief Privacy Officer that contains the following information:
  - description of the breach or suspected breach
  - action taken by the Director or OAIC officer to address the breach or suspected breach
  - the outcome of that action, and
  - the Director’s reasons for their view that no further action is required
- save a copy of that email in the following TRIM container:
  - Data Breach Response – reports and investigation of data breaches within the OAIC [internal link redacted].

**OAIC Data Breach Response 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. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or a human resources adviser.

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

**STEP 1: Contain the breach**

**STEP 2: Assess the risks associated with the breach**

**STEP 3: Consider breach notification**

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

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, the response team should consider whether remedial action can be taken to reduce any potential harm to individuals.

The response team should refer to the checklist below and to the OAIC’s *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, which provides further detail on each step.

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.

Following serious data breaches, the response team should conduct a post-breach review to assess the OAIC’s response to the breach and the effectiveness of this plan and report the results of the review to the OAIC Executive. The post-breach review report should identify any weaknesses in
this response plan and include recommendations for revisions or staff training as needed. As part of the review the response team should refer to the OAIC’s Guide to securing personal information.

The response team should also consider the following documents where applicable:

- OAIC Business Continuity Plan
- ICT Incident Response Plan
- ICT Disaster recovery plan

**Testing this plan**

Members of the response team should test this plan with a hypothetical data breach 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 OAIC Executive on the outcome of the test and make any recommendations for improving the plan.

**Records management**

Documents created by the response team, including post-breach and testing reviews, should be saved in the following TRIM container:

- Data Breach Response – reports and investigation of data breaches within the OAIC [internal link redacted]

**Reporting**

The OAIC’s privacy management plan states that the internal handling of personal information will be an agenda item on the Executive group meetings at least once each quarter and include a report of any privacy complaints against the OAIC and internal data breaches.

The Assistant Commissioner Dispute Resolution should liaise with the Chief Privacy Officer on the preparation of reports on internal data breaches.
OAIC’s Data Breach Response Check List

Step 1: Contain the breach

☐ Notify the Chief Privacy Officer, who may convene 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.
  ☐ Consider whether TRIM/Resolve systems administrator needs to be advised.

☐ Consider whether team needs other expertise

☐ Inform the OAIC Executive, including the Australian Information Commissioner, as soon as possible; provide ongoing updates on key developments.

☐ Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the OAIC to take appropriate corrective action.

☐ 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 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 context of the information 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.

- Determine whether and how to notify affected individuals. Does the breach trigger the requirements of the NDB scheme – is the breach likely to result in serious harm to any of the individuals to whom the information relates and the OAIC 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 NDB scheme is triggered – a formal notification to the AIC through the OAIC’s NDB form should be completed and registered in Resolve. Even if the NDB scheme threshold is not met would notifying the individuals be appropriate?

- Consider whether others should be notified, including the ACSC, 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 OAIC is contractually required or required under the terms of an MOU 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 handling that contributed to the breach

- Conduct a post-breach review and report to OAIC 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.
Responding to a data breach

**STEP 1:**
Contain the breach

**STEP 2:**
Assess the risks for individuals associated with the breach

**STEP 3:**
Consider breach notification

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