DATA BREACH RESPONSE PLAN

A data breach occurs when personal information 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 HRCAV including information stored on the HRCAV database managed by a third party provider. 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 HRCAV 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. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

Any data breaches are to be reported to the Chief Administrative Officer

Some data breaches may be comparatively minor, and able to be dealt with easily.

For example, a staff member 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, no further action may be required.

An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
2. this is likely to result in serious harm to one or more individuals, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action

The CAO should use their discretion in determining action required to address the data breach. In making that determination, the CAO should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a risk of serious harm to any of the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in HRCAV 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 CAO must immediately notify the Executive Committee and take appropriate action to address the breach. The checklist below sets out the steps to be taken in the event of a serious data breach.

Minor data breaches are to be recorded by the CAO. Include:

- description of the breach or suspected breach
- action taken by the staff member to address the breach or suspected breach
- the outcome of that action, and
- the CAO's reasons for their view that no further action is required

HRCAV 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 CAO 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

Steps 1, 2 and 3 should be taken 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, 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 CAO should conduct a post-breach review to assess the response to the breach and the effectiveness of this plan and report the results of the review to the Executive Committee. 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.

DATA BREACH RESPONSE CHECK LIST

Step 1: Contain the breach

- Notify the CAO, who will coordinate the response.
- Take action to ensure that the breach is immediately contained. As required, liaise with
  - Event Secretary
  - Proactive Technology Partners
- Inform the Executive Committee,
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or to assist in taking appropriate corrective action.

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 HRCAV 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. Even if the NDB scheme threshold is not met would notifying the individuals be appropriate?
- Consider whether others should be notified, including the police/law enforcement, or other agencies or organisations affected by the breach.

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
- Complete an assessment within 30 calendar days after the day the HRCAV became aware of the grounds (or information) that caused it to suspect an eligible data breach
- Conduct a post-breach review and report to the Executive Committee 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

Relevant Documents:

- HRCAV Privacy Policy
- HRCAV Database Policy