OPERATIONAL PROCEDURE

Data Breach Response Plan

Overview

This Data Breach Response Plan (response plan) provides instructions for PIA employees in the event of a data breach, or suspected data breach, and includes contact details for key personnel and roles and responsibilities.

The response plan is intended to help PIA contain, assess and respond to data breaches in a timely fashion and mitigate potential harm to affected individuals.

A data breach is when personal information held by PIA is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. This could be due to malicious actions (hacking or phishing), or by accident (personal information sent to the wrong person, or a device containing personal information is stolen).

Personal information is information or an opinion, true or false and whether recorded in a material form or not, about an identified or reasonably identifiable individual. For example, at PIA this information includes names, addresses, dates of birth, email addresses, membership status, banking details, employee records, and more.

Data Breach Response Team

PIA's Data Breach Response Team includes:

- Chief Executive Officer
- National Finance Manager
- Executive Assistant to the CEO (Response Team Coordinator)
- Membership & On-line Services Manager

More information about the Response Team is at step 4.

Implementation

1. A data breach occurs or is suspected

Discovered by an employee, or PIA otherwise alerted.

2. Employee immediately:

2.1 Notifies their manager of the suspected breach.

2.2 After notifying the manager, records and provides their manager with the following details, if possible:

- Time and date the suspected breach was discovered
- Type and quantity of personal information involved
- Cause and extent of the breach
- Circumstances surrounding the information and the breach.

3. Manager immediately:

3.1 Determines if a breach has or may have occurred.

3.2 Determines if the breach is serious enough to escalate to the Data Breach Response Team, or if it is appropriate to handle at manager level (see figure 1 for assistance with this decision).

3.3 If the breach is serious enough, escalate immediately to the Data Breach Response Team by emailing all information about the situation to all Response Team contacts listed below, and speak to the Chief Executive Officer (or their delegate).

Figure 1

Should it be escalated?

Some data breaches may be minor enough to be managed without action from the Data Breach Response Team (Response Team). Managers should consider:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or could there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in PIA's processes, procedures or systems?
- 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 breach should be escalated.

An example of a minor breach that does not need to be escalated is an employee accidentally emailing some personal information to a recipient outside of PIA who is not authorised to receive the information. The manager would consider the sensitivity of the content, if the email can be recalled or if the recipient can be contacted and can confirm they have deleted the email. In this case there may be no reason to escalate the issue to the Response Team.

An example of a breach that should be escalated is an employee emailing some personal information to someone pretending to be a PIA employee (a phishing attack).

Reporting minor breaches

Even if a manager decides not to escalate a minor breach, they should send a report about the breach and how it was handled to the Response Team Coordinator. The report can be in the form of an email and should contain:

- A description of the breach or suspected breach
- Action taken by the manager or their staff to address the breach
- Outcome of the action
- Manager's view that no further action is required.

The Response Team Coordinator should collate the report in the data beach report folder and add the event to the data breach register.

4. Data Breach Response Team (Response Team)

4.1 The Response Team includes:

Chief Executive Officer
National Finance Manager
Executive Assistant to the CEO (Response Team Coordinator)
Membership & On-line Services Manager

The Response Team can contain fewer or more members but should always include the Chief Executive Officer. The Team may engage outside experts as required such as legal advisors and forensic investigators.

4.2 A swift response can mitigate potential harm. The Response Team can act immediately by taking common sense steps to contain the breach (see Step 1 below).

5. Data Breach Response Process

5.1 Data breaches must be handled on a case-by-case basis according to the level of risk the breach presents.

5.2 These are the steps to follow when responding to a breach or suspected breach. Ideally steps 1-3 should be done simultaneously or in quick succession:

STEP 1: Contain the breach and do a preliminary investigation
STEP 2: Assess the risks associated with the breach
STEP 3: Notify the relevant internal and external persons and/or agencies
STEP 4: Review the breach and actions taken to rectify the breach

Steps can be combined, some may not be required, and additional steps may be taken depending on the nature of the breach.

The Response Team should refer to the Office of the Australian Information Commissioner's (OAIC) *Data breach notification: a guide to handling personal information security breaches* for further detail on each step. A process is provided below to guide the Response Team.

Remember to:

a. Preserve evidence.
b. Keep appropriate records about the breach, including steps taken and decisions made.
c. If law enforcement is involved, consult them before making any media statements.

STEP 1: Contain the breach and do a preliminary investigation

- **Take whatever steps possible to immediately contain the breach.** For example, shut down the system that was breached, remove unauthorised system access, stop unauthorised processes, recover the information, address weakness in physical or electronic security and alert all PIA employees to be on alert for suspicious contact or use of information.

  Preserve evidence that may be valuable in determining the cause of the breach or allowing further investigation to be done, such as an original phishing email from a malicious address.

  Consider suspending duties and access rights of employees involved in the breach to limit their ability to potentially interfere with investigations or data and prevent them from trying to remedy the situation without authorisation. This protects them against claims of the same. An accidental data breach can be a traumatic experience for employees involved.

- **Determine if any immediate steps (remedial action) can be taken to mitigate potential harm an individual might suffer as a result of a breach and action these steps.** For example, reset member login passwords if those passwords were part of the breach.

- **Investigate.** Quickly appoint someone who has enough authority to lead an investigation and involve other employees or PIA volunteers as necessary. This person should gather any necessary information and make initial recommendations. Collect the following information:

  - The date, time, duration, and location of the breach
  - The type of personal information involved
  - How the breach was discovered and by whom
  - The cause and extent of the breach
  - A list of affected, or possibly affected, individuals
  - How the breach can be contained

- **Seek expert advice**. Engage a lawyer and/or forensic investigator or specialist. Contact PIA's insurer to advise of the situation and check any obligations we have under our insurance policies.

STEP 2: Conduct a reasonable assessment of the risks associated with the breach

- **Consider the following factors in assessing the risks, and document the findings and decisions as follows:**
    - The type of personal information involved, and persons affected by the breach
    - The sensitivity of the information
    - Whether the information is protected by security measures, and the likelihood that the security measures could be overcome
    - The persons or kinds of persons who have obtained or could obtain the information
    - If the persons or kinds of persons who obtained or could obtain the information would have the knowledge or means of decrypting or unlocking any protection the breached information carries (such as the encryption key relating to encrypted information)
    - The cause and extent of the breach
    - Whether the context of the information is important
    - The nature of harm that could potentially be caused to affected individuals by the breach
    - **Whether the breach is likely to result in serious harm** to any individual(s) whose data was breached
    - If any remedial action has, or could, be taken, and its effect
- If there is remedial action that should be taken, action it.
- **If PIA has reasonable grounds to believe that the breach is likely to result in serious harm to any of the individual(s) whose data was breached, PIA must notify affected individuals and the OAIC in step 3**, unless remedial action has been successful in making serious harm no longer likely.
- If PIA only has grounds to suspect that the breach is likely to result in serious harm to any of the individual(s) whose data was breached, PIA should **expeditiously** and within 30 days, conduct this assessment. If the assessment will take longer than 30 days, documentation will be required as to why that is the case.

STEP 3: Notify the relevant internal and external persons and/or agencies.

- **Notify** PIA's National President, and the Chair of the Finance, Audit and Risk Management Committee.
- **Notify** the police if the breach appears to involve criminal activity such as theft.
- **If there is a likely risk of serious harm to the affected individuals, they must be notified together with the OAIC.** Sometimes it may be appropriate to notify affected individuals early in the process if they are at immediate serious risk. PIA has three notification options:
    - **Option 1:** Notify all individuals
    - **Option 2:** Notify only those individuals at risk of serious harm.
    - If Option1 and 2 are not practicable, then **Option 3:** Publish a statement on the PIA website and publicise it.

  Consult with PIA's legal advisor regarding the content of such notification prior to sending it.

  Choose a method of notifying individuals after considering the likelihood of those persons being made aware using such method.

  It may be appropriate to notify affected individuals even if they are not at serious risk but would otherwise reasonably expect to be notified in the situation at hand.

  The minimum information to be reported to individuals and the OAIC is the same and is:

    - PIA's name and contact details
    - A description of the eligible data breach
    - The kind of kinds of information involved in the eligible data breach
    - What steps we recommend individuals take in response to the eligible data breach.

  The OAIC provides an electronic form to notify them of eligible data breaches. https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

STEP 4: Review the breach and actions taken to rectify the breach

- **Fully investigate the cause of the breach.**
- **Consider processes and procedures to reduce the risk of future breaches.** Refer to the OAIC's *Guide to securing personal information* for steps and strategies.
- It may be relevant to report the breach to ASIC, APRA, the ATO, or the Australian Cyber Security Centre.
- **Provide a report to the Board or Finance, Audit and Risk Management committee.** The report may include recommendations such as updating security systems or procedures, updating policies or revising employee training practices.
- **Response Team Coordinator** to ensure all records are saved in the data beach report folder and add the event to the data breach register.

Review

The response plan should be tested with hypothetical examples and reviewed in the sooner of these circumstances:

- Every two years, or
- Coinciding with introduction of new products or services, system upgrades, other events involving handling of personal information.

Related Documentation and Resources

PIA's Data Breach Register
Office of the Australian Information Commissioner's Website
OAIC's Notifiable Data Breach Scheme Flowchart

Version Control

Authorising Entity:	Board

Version	Author	Revision Notes	Date Approved
1	Brenda Payne	Original Document	22 February 2018 Re-approved 7 July 2020