Data Breach Response Procedure

CONTENTS

1 Purpose 1
2 Scope 1
3 Policy statement 1
4 Procedures 1
5 Responsibilities 5
6 Definitions 6
7 Related legislation and documents 7
8 Feedback 7
9 Approval and review details 7

1 Purpose

This procedure outlines the actions to be undertaken should a data breach occur and, where considered an eligible data breach under the National Data Breach Scheme, when to notify individuals and the Office of the Australian Information Commissioner (OAIC) of the breach.

2 Scope

This procedure governs suspected data breaches and applies to all PIA staff, affiliates, students, contractors and any other third party who collects or manages personal information on behalf of the organisation.

3 Policy statement

It is the aim of PIA to be more resilient to data breaches and cyber-attacks and better able to protect its interests in the digital environment. The organisation recognises the importance of cyber security and as such, it is committed to ensuring all activities involving information technology are appropriately defended against cyber security threats and data breaches.

This policy supports the Board of Directors and its committees in demonstrating that cyber security risks and measures are being identified and managed in a way that is appropriate for the organisation in trying to meet its business objectives.

4 Procedures

4.1 Suspected data or privacy breach

Access to personal information is granted to staff only where this is necessary for work purposes and staff must only access personal information if there is a work related reason for this. Personal information must be protected against loss, unauthorised access or modification, disclosure or misuse.

A suspected data breach is considered to be any event which may have involved unauthorised access, unauthorised disclosure or loss of data involving personal.

4.2 Reporting a suspected data breach

If a staff member becomes aware of a suspected data breach, they are to contact the Information Privacy Officer (in this case, the PIA Registrar) as soon as possible with as much information as is available via:

Email: registrar@PIA.edu.au
Phone: 02 8319 8202

The information to be provided includes:

- the time and date the suspected data breach was discovered,
- the type of personal information involved,
- the cause and extent of the breach,
- the context of the affected information and the breach, and
- the actions undertaken to contain the breach (see clause 5).

PIA only has thirty (30) days from becoming aware of the breach, to carry out a reasonable and expeditious assessment as to whether there are reasonable grounds to believe that the data breach has been an eligible data breach.

4.3 Notification requirements of eligible data breaches

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

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that PIA holds;
- this is likely to result in serious harm to one or more individuals; and
- the organisation has not been able to prevent the likely risk of serious harm with remedial action.

Whether a data breach is likely to result in serious harm requires an objective assessment by the Information Privacy Officer based on information immediately available or following reasonable inquiries or an assessment of the data breach. The potential kinds of harms that may follow a data breach include:

- identity theft,
- significant financial loss by the individual,
- threats to an individual's physical safety,
- loss of business or employment opportunities,
- humiliation, damage to reputation or relationships, and/or
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

If PIA acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the OAIC.

If personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

4.3 Once a breach is declared eligible

If a data breach is declared eligible by the Information Privacy Officer, the organisation's CEO is to be notified and a critical incident report is actioned.

The organisation is required to prepare a statement and provide a copy to the OAIC. The statement is to include the name and contact details of the organisation, a description of the eligible data breach, and what steps the organisation recommends to individuals at risk of serious harm in response to the eligible data breach.

4.4 Data Breach Response Procedure

PIA's Data Breach Response Procedure comprises four steps (consistent with the OAIC guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)).

Each data breach response needs to be tailored to the circumstances of the incident.

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the OAIC if required.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

Data Breach Response Procedure

Step 1 - Contain	Once a data breach is suspected immediate action must be taken to limit the breach. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security. To identify strategies to contain a data breach consider: • How did the data breach occur? • Is the personal information still being shared, disclosed, or lost without authorisation? • Who has access to the personal information? • What can be done to secure the information , or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals? Notify the Information Privacy Officer. During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.

Step 2 - Assess	An assessment of the data breach will identify the risks posed by a data breach and how these risks can be addressed and must be conducted as expeditiously as possible by the Information Privacy Officer based on the information available and in consultation with the COO / IT Manager. The aim is to understand the risk of harm to affected individuals, and identify and take all appropriate steps to limit the impact of a data breach. Considerations in this assessment include: • the type or types of personal information involved in the data breach; • the circumstances of the data breach, including its cause and extent; and • the nature of the harm to affected individuals, and if this harm can be removed through remedial action. Remedial action to reduce any potential harm to individuals should be taken (such as recovering lost information before it is accessed). Contain. The Information Privacy Officer is to determine whether the data breach is an eligible breach under the NDB scheme. This assessment is to occur within 30 days and determined in accordance with the criteria for assessing a data breach, including the risk of harm and remedial action. If it is an Eligible Data Breach, the CEO will convene the Notifiable Data Breach Response Team (or the Critical Incident Team in accordance with the Critical Incident Policy and Procedure) for steps 3 and 4.
Step 3 - Notify	Notification to affected individuals may be considered for data breaches but must be undertaken for eligible data breaches under the NDB Scheme. Notification can be an important mitigation strategy that has the potential to benefit both PIA and the individuals affected by a data breach. However, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required. In considering to notify individuals who may be impacted by a data breach the following should be considered: • what information is provided in the notification and how this will be provided; • who is responsible for notifying individuals and creating the notification; • who else other than affected individuals (and the OAIC if the notification obligations of the NDB scheme apply) should be notified; • where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public; and • whether the incident triggers reporting obligations to other entities (eg TEQSA or the Australian Taxation Office). Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of the organisation. Notification has the practical benefit of providing individuals with the opportunity to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible

	scams resulting from the breach. Individuals who have been affected by a data breach must be dealt with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification may also serve to demonstrate that privacy protection is taken seriously. The decision to notify will be made by the CEO in consultation with the Notifiable Data Breach Response Team as necessary. If it is an eligible data breach, notification options include: • Option 1: Notify all individuals whose personal information was part of the eligible data breach and would be used when PIA cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but serious harm is likely for one or more of the individuals. • Option 2: Notify only those individuals at risk of serious harm. • Option 3: Publish notification If neither option 1 or 2 above are practicable, for example, if the entity does not have up-to-date contact details for individuals, this may include providing a copy of the statement on the website and take reasonable steps to publicise the statement.
Step 4 - Review	A Critical Incident Report will be completed on an eligible data breach incident to improve personal information handling practices. This might involve: • a security review including a root cause analysis of the data breach; • a prevention plan to prevent similar incidents in future; • audits to ensure the prevention plan is implemented; • a review of policies and procedures and changes to reflect the lessons learned from the review; • changes to staff selection and training practices; and • a review of service delivery partners that were involved in the breach. The intent of the Critical Incident Report is to strengthen the PIA's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures. If any updates are made following a review, staff will be notified in any changes to relevant policies and procedures to ensure a quick response to a data breach.

The diagram in **Attachment A** summarises the data breach response procedure in accordance with the OAIC *Data Breach Preparation and Response* Guide. The parts of this process that are required by the NDB scheme are coloured red.

5 Responsibilities

- The Information Privacy Officer is to assume responsibility for alerting the CEO as soon as possible who, in turn, will re-assess the situation and convene a Critical Incident Team if deemed necessary. It is also the responsibility of the Privacy Officer to participate in regular training webinars as provided by the OAIC in relation to the Notifiable Data Breaches scheme.

- COO/ IT Manager is to establish the cause and impact of a breach involving PIA's IT facilities and services.
- Quality Assurance and Risk Committee is to assess the risks from the breach and ensure it has been dealt with in a sustainable way.
- Users of IT Facilities and services have the following responsibilities:
  - using IT facilities and services according to IT policies at all times;
  - being aware of the security requirements of the IT facilities and services they use, and take every precaution to safeguard their access to these systems against unauthorised use; and
  - immediately reporting any known or suspected security incidents and breaches to the COO/IT Manager.

6 Definitions

Eligible data Breach: The *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth),* also referred to as the Notifiable Data Breaches (NDB) Scheme amends the *Privacy Act 1988 (Cth)* (the Commonwealth Privacy Act), and in the instances where the NDB Scheme applies to PIA, there is a mandatory requirement for PIA to notify the Commonwealth Privacy Commissioner and affected individuals of 'eligible data breaches'. An eligible data breach occurs if:

1. there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity;
2. the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates; and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

Harm: Data breaches can cause significant harm in multiple ways. Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation. Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

Loss of data: Loss refers to the accidental or inadvertent loss of personal information held by the organisation, in circumstances where is it is likely to result in unauthorised access or disclosure. For example, where a staff member leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.

Unauthorised access: Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, a staff member browses a student academic or personal record without any legitimate purpose.

Unauthorised disclosure: Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity. For example, as staff member accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.

7 Related legislation and documents

This document is based on the Office of the Australian Information Commissioner (OAIC) Data Breach Preparation and Response Plan (July 2019).

Information Technology Usage Policy and Procedures
Privacy and Personal Information Policy and Procedure
Records Management, Security, Retention and Disposal Policy and Procedure
Risk Management Policy
Risk Management Framework
Staff Code of Conduct
Student Code of Conduct and Disciplinary Procedures

8 Feedback

PIA staff and students may provide feedback about this document by emailing policy@pia.edu.au.

9 Approval and review details

Approval and Review	Details
Approval Authority	Board of Directors
Administrator	COO / IT Manager

Attachment A: Data breach response procedure