Procedure: Data Breach Management

Purpose

This Data Breach Management Procedure sets out the procedure for our staff where thinkstep-anz experiences a data breach (or suspects that a data breach has occurred). It should be read in conjunction with our Information Security Policy.

This procedure applies to all persons employed at thinkstep-anz, and external organisations and their personnel who have been granted access to our IT infrastructure, services, and data.

Background

A data breach occurs where:

- there is a failure that has caused or has the potential to cause unauthorised access to thinkstep-anz data
- personal information held by thinkstep-anz is lost or subjected to unauthorised access, modification, use or disclosure or other misuse or interference
- confidential information is unlawfully used or disclosed. This includes a broader range of information than personal information as it includes information about all entities, not just individuals.

This procedure:

- sets out the roles and responsibilities of staff
- provides the details of appropriate staff to be contacted in the event of a data breach
- outlines the procedure to be followed in the event of a data breach

Procedure

1. Initial response

A staff member who has identified a suspected data breach should immediately notify the Manager responsible for the data subject to the breach.

The notification must include information about the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and breach.

2. Responsible manager to assess breach

The Responsible Manager will assess and determine whether a data breach has occurred. If it is determined that a breach has occurred, the Privacy Officer must be immediately advised.

The Responsible Manager will follow the Data Breach Response Process (Appendix A) in consultation with the Privacy Officer and where it is determined that the breach is not a serious, eligible or notifiable breach a Data Breach Assessment Report (Appendix B) will be completed and any remedial action undertaken within 30 days.

3. Response team to convene

Where it is suspected that the data breach may be a serious, eligible or notifiable data breach, the Response Team must be convened.

Membership of the Response Team includes the Chief Executive Officer, Privacy Officer, IT Manager, and any other appropriate staff as determined by the Privacy Officer.

The Response Team is responsible for decisions regarding notification of individuals who have been impacted in the data breach. The Response Team will consider the following factors:

- the risk of harm to the individual/organisation
- measures that thinkstep-anz has taken to avoid or remedy any actual or potential harm
- the ability of thinkstep-anz to take further steps to avoid or remedy harm
- whether the information that has been compromised is sensitive, or likely to cause humiliation or embarrassment for the individual/organization
- whether there are any applicable legislative provisions or contractual obligations that require thinkstep-anz to notify affected individuals or other parties.

The incident must be recorded on a Data Breach Assessment Report.

If the breach is determined to be serious, eligible or notifiable data breach, it must be managed according to the Data Breach Response Process and this Procedure.

4. Serious, eligible and notifiable data breach response

Once the breach has been determined to be a serious, eligible or notifiable breach, the process outlined below shall be followed. The Response Team will undertake an assessment of the risks involved and use that risk assessment as the basis for what actions to take in the circumstances. Each breach will need to be dealt with on a case-by-case basis.

The Response Team shall follow the Data Breach Response Process (Appendix A) outlined below:

- Step 1: Contain the breach and conduct a preliminary assessment

  Once a data breach has been identified, action must be taken to immediately contain it. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached.

  The Privacy Officer will be responsible for leading the initial investigation. Where the Privacy Officer is unavailable, another person who is most suitably qualified to carry out the initial investigation shall be appointed by the Chief Executive Officer.

  The following questions shall be addressed as part of the preliminary assessment:

  - what information does the breach involve?
  - what was the cause of the breach?
  - what is the extent of the breach?
  - what are the harms (to affected persons/organisations) that could potentially be caused by the breach?
  - how can the breach be contained?

- Step 2: Evaluate the risks associated with the breach

  The following factors are relevant when the Response Team assesses the risk:

  - the type of information involved
  - whether it is personal information or protected thinkstep-anz information
  - whether the type of information has been compromised creates a risk of greater harm
  - who is affected by the breach

  The Response Team shall establish the cause and extent of the breach by considering:

  - risk of ongoing breaches or further exposure of the information
  - evidence of theft
  - is the information adequately encrypted, anonymised or otherwise not accessible?
  - the source of the breach (risk of harm may be lower where source of the breach is accidental rather than intentional)
  - has the information been recovered?
  - steps already been taken to mitigate the harm
  - whether the problem is systematic or an isolated incident
  - how many persons are affected by the breach

  The Response Team shall assess the risk of harm by considering:

  - who the recipient of the information is
  - what harm to persons could result from the breach
  - what other possible harms exist (e.g. loss of trust/reputational damage, legal liability)

- Step 3: Notification

  If the Response Team determines that the data breach creates a real risk of serious harm to a person, the affected person or entity should be notified.

  The Response Team shall assess the risk of serious harm to affected individuals or entities by considering:

  - the risk of serious harm to the person as determined by the evaluation of the risk/s associated with the breach
  - the ability of the affected person or entity to avoid or mitigate possible harm if notified of a breach
  - the likelihood of the information that has been compromised to cause humiliation or embarrassment
  - the legal and contractual obligations to notify and what are the consequences of notification

The Response Team shall notify the affected person/entity as soon as reasonably possible. Notification shall be made by phone, letter, email or in person.

The content of the notification may include, where relevant:

- incident description and type of information involved
- thinkstep-anz's response to the breach
- thinkstep-anz's contact details
- whether the breach has been notified to other external contact(s) and the legal implications

The Response Team will also determine if it is appropriate and necessary to notify other third parties, such as:

- the Police
- insurance providers
- credit card companies and/or financial institutions
- professional or other regulatory bodies
- other internal or external parties who have not already been notified
- agencies that have a direct relationship with the information lost/stolen

Where the breach is determined to be an eligible data breach under the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (AU)* (NDB scheme), the Response Team will also submit a statement to the Australian Information Commissioner in the appropriate form.

Where the breach is determined to be a notifiable privacy breach under the *Privacy Act 2020 (NZ)*, the Response Team will notify the New Zealand Privacy Commissioner within 72 hours.

- Step 4: Prevention of future breaches

  Once immediate steps have been taken to mitigate the risks associated with a breach, the Response Team must take the time to fully investigate the cause of the breach.

  A brief shall be prepared for the Chief Executive Officer, detailing the outcome of the investigation and providing any relevant recommendations, including:

  - making appropriate changes to policies and procedures if necessary
  - revising staff training practices if necessary
  - updating this Data Breach Management Procedure if necessary

Assessment and responsibility

Where the data breach is not a serious data breach, the Responsible Manager will conduct the Data Breach Response Process in consultation with the Privacy Officer.

Where the data breach may be a serious, eligible or notifiable data breach, the Response Team will convene in accordance with the Data Breach Management Procedure.

The Chief Executive Officer must be advised of any potential serious data breach by the Privacy Officer or their delegate.

Compliance, monitoring and review

thinkstep-anz will regularly review, develop, maintain, and test its systems and procedures to support data security and this Policy.

Suspected breaches or misuse of this policy are to be reported to the Chief Executive Officer. Alleged breaches of this policy shall be dealt with by the processes outlined for breaches of the Code of Conduct.

In this procedure

A **data breach** may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. Examples of data breach include but are not limited to:

- a device containing data is lost or stolen
- paper files or records containing data are lost or stolen
- a database is hacked, or malware infects data or information systems
- data is provided to the wrong person
- data or information systems are used, accessed, or modified without permission
- users with permission look up data or information for unauthorized purposes
- data is posted on a website without permission
- a user account is compromised
- failed or successful attempts are made to gain unauthorized access to data or information systems
- information systems or their protections fail or become unavailable
- data is not disposed of securely and becomes public

An **eligible data breach** (*NDB Scheme AU*) arises when the following 3 criteria are satisfied:

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

A **notifiable data breach** (*Privacy Act 2020 (NZ)*) is one in which an organisation has reasonably judged that a breach it has experienced either has caused or is likely to cause someone serious harm.

Responsible Manager means the Manager responsible for the data subject to the breach.

Response Team means the Chief Executive Officer and IT Manager, and any other appropriate staff as determined by the IT Manager.

Serious data breach means a data breach that is likely to result in **serious harm** to any individual or organisation, which may include, but is not necessarily limited to, serious financial, physical, psychological, emotional, or reputational harm. Examples of serious harm include:

- financial fraud including unauthorized credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- significant commercial or reputational damage due to release of commercially sensitive information

Accountabilities	
Privacy Officer	Barbara Nebel
IT Manager	Matthias Nebel
Supporting Information	
Legislation	*Privacy Act 1988 (Cth)* *Privacy Amendment (Notifiable Data Breaches) Act 2017* *Privacy Act 2020 (NZ)*
Parent Document	Information Security Policy

Signed By: **Date:**

Printing this procedure

All official procedures are updated electronically and available on our website. Before relying on a printed copy please check that you have the latest version.

Related policies:

- Code of Conduct
- Privacy Policy
- Information Security Policy

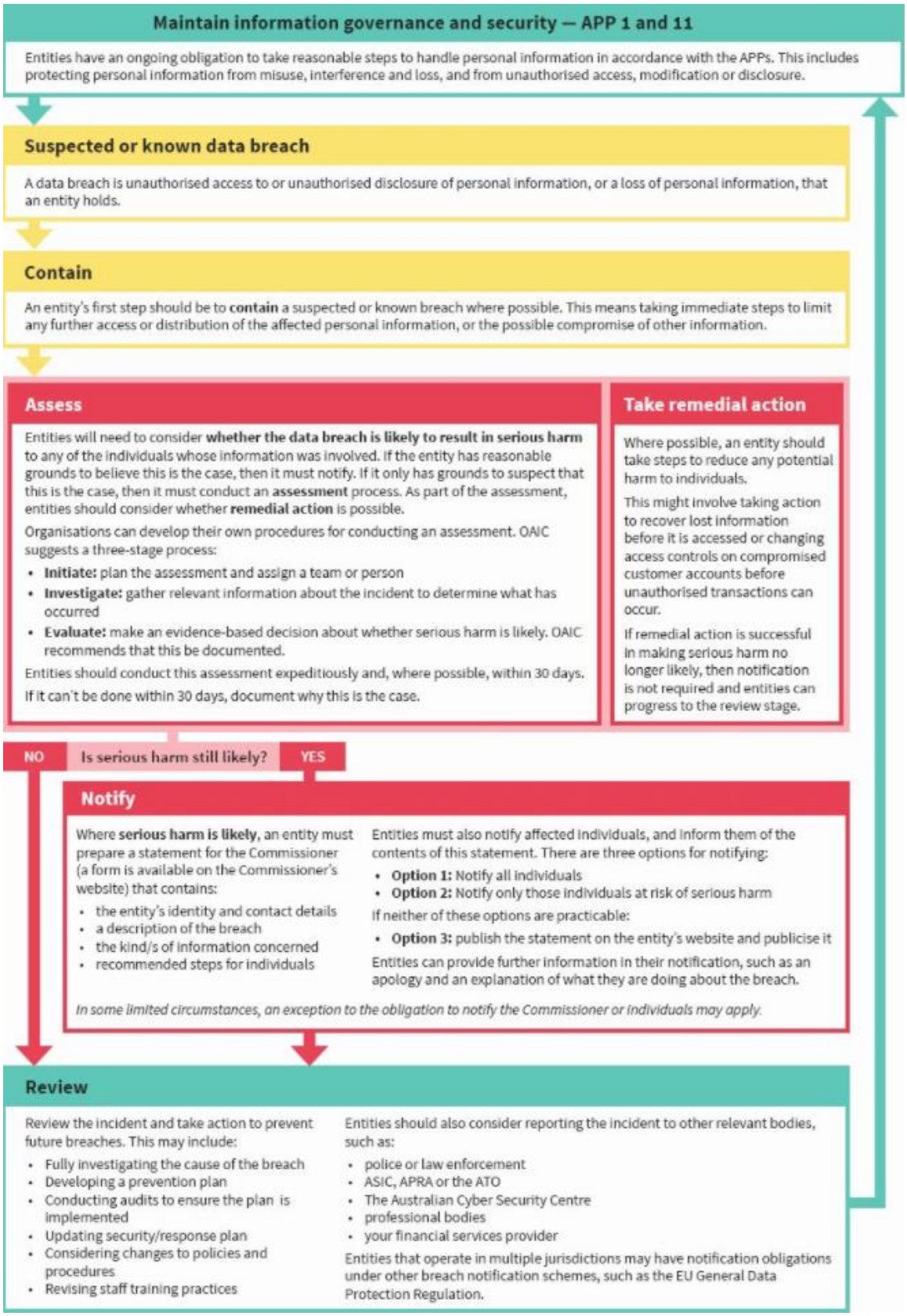
Document information

Date:	3/12/2021
Version:	B - Draft
Review date:	Annual
Project sponsor:	Barbara Nebel
Author:	Andrea Davies / Sarah Cooper
Approved:	Barbara Nebel
Sensitivity:	Restricted

Version control

Version	Date	Changes	Author	Reviewer
1	6/12/2021	Final version released	AD/SC	BN

Appendix A – Data Breach Response Process



(Reproduced from Office of the Australian Information Commissioner)

Appendix B – Data Breach Assessment Report

thinkstep-anz Data Breach Assessment Report

Description	Details
Description of the breach	[Short description of the breach, including the date and time the breach was discovered and the duration and location of the breach]
Type of information involved	[Type of information involved]
How the breach was discovered	[Details about how the breach was discovered, and by whom]
Cause and extent of breach	[Details about the cause and the extent of the breach]
List of affected individuals	[List the affected individuals, or describe the class of individuals who are or may be affected by the data breach]
Is the breach likely to result in serious harm to any of the individuals to whom the harm relates?	[Evaluate whether the breach is likely to result in serious harm to any of the individuals to whom the information relates, having regard to: - the kind of information involved; - the sensitivity of the information; - whether the information is protected by one or more security measures, and the likelihood of those measures being overcome; - the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and - if a security technology or methodology was used in relation to the information and designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that persons could circumvent the security technology or methodology]
Remedial action	[Details of the steps thinkstep-anz has taken to reduce any potential harm to individuals, e.g. by recovering lost information before it is accessed or changing access controls on compromised systems]
Is or will the remedial action result in making serious harm no longer likely?	[State whether the remedial action will result in making serious harm no longer likely. If serious harm is no longer likely, thinkstep-anz is not required to prepare a statement to the Australian or New Zealand Information Commissioner / Privacy Commissioner or to notify affected individuals]
Who will be notified of the breach?	**[Select one of the following options]** **[Option 1]** thinkstep-anz has determined that the data breach is likely to result in serious harm to individuals and therefore the thinkstep-anz will: - provide a statement to the relevant Information Commissioner / Privacy Commissioner containing a description of the breach, the kind of information concerned and the recommended steps for individuals.

	- will [*select one of the following options*] notify all affected individuals / notify affected individuals at risk of serious harm impracticable] **[Option 2]** thinkstep-anz has determined that notification of the data breach is not required because it is not likely to result in a serious risk of harm to any individuals.
Preliminary recommendations	[Include any recommendations on actions that could be undertaken to contain the breach, remediate the breach or prevent future breaches of a similar nature – these recommendations will feed into thinkstep-anz's comprehensive review of the data breach]
Names of response team members	[Insert the names and roles of Response Team members. Members of the Response Team may include the Chief Executive Officer, Privacy Officer, IT Manager, and any other appropriate staff as determined by the Privacy Officer having regard to the skills required to respond to the breach]
Date	[Insert date]