



Notifiable Data Breach Policy and Procedure

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	Notifiable Data Breach Policy and Procedure
Document Title	Notifiable Data Breach Policy and Procedure
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

1. Purpose

The purpose of this policy and procedure is for the Company to meet expectations for accountability and transparency in data breaches by providing a system to prevent and manage data breaches.

2. Scope

This policy and procedure applies to all Company staff.

3. Definitions

Term	Definition
eligible data breach	occurs when there is loss of, unauthorised access to, or unauthorised disclosure of, personal information, which is likely to result in serious harm, and remedial action has not been taken to prevent such risk of harm.
Business Unit Manager	is the person holding the position of Business Unit Manager as appointed by the Company.
data breach	is an unauthorised access or disclosure of personal information, or loss of personal information. Examples of data breaches may include but are not limited to: • loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information; • unauthorised access to personal information by an employee. • inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person. • disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures. • compromised data systems.
data breach response plan	is described in clause 5.
NDB scheme	is contained in Part IIIC of the Privacy Act and applies to data breaches that occur on or after 22 February 2018.
personal information	is information about an identified individual, or an individual who is reasonably identifiable, including information that is not about an individual on its own that can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.
response team	a response team will consist of the Business Unit Manager, except where he/she was responsible for (or involved in) the breach, who is responsible for leading the response team, and the relevant Company nominee(s) and appropriate other staff.

serious harm	• financial fraud including unauthorised credit card transactions or credit fraud; • identity theft causing financial loss or emotional and psychological harm;
--------------	--

4. Policy

The Company acknowledges it has a responsibility to protect personal information and adopts the principles contained within the Privacy Act for the handling of personal information designed to lower the risk of a data breach occurring and to effectively reduce the impact of a data breach. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The Company will enact a data breach response plan to reduce reputational impact of a data breach by minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm, and demonstrates that the Company takes its responsibility to protect personal information seriously, which is integral to building and maintaining trust in its personal information handling capability.

5. Procedure

The Data Breach Response Plan is a four-step process — contain, assess, notify, and review:

Contain- Contain the data breach to prevent any further compromise of personal information. Notify the Business Unit Manager, who will convene the response team. If the Business Unit Manager has had prior involvement with the breach, then the Global Head of Enterprise Technology will lead and convene the response team. Ensure evidence is preserved that may be used to determine the cause of the breach. Consider a communications strategy. The Business Unit Manager will report the breach to the CEO and the Risk and Compliance team as soon as possible.

Assess- The response team will be responsible for initiating, and recording results of, an assessment of the data breach; gathering all relevant information; and evaluating whether serious harm has occurred based on available evidence. The response team should complete the assessment as soon as possible after the notification of the breach and within 30 days. The response team will conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm, and as a result require notification. They will investigate and record the date, duration, time and location of the breach, and collect information of how and by whom the breach was discovered; and the cause and extent of the breach. An assessment of a suspected data breach should consider whether remedial action is possible.

Where remedial action is considered possible the Company will move to reduce any potential harm to individuals. This may include the recovery of lost information before it is accessed or changing access controls on compromised accounts before unauthorised transactions can occur. If remedial action is successful and serious harm is no longer likely, then notification (under 3

below) is not necessary.

Notify- When the Company is aware that there are reasonable grounds to believe that there has been an eligible data breach, it will notify the Office of the Australian Information Commissioner (Commissioner) and affected individuals. Notifications to the Commissioner should be lodged through a Notifiable Data Breach form, in accordance with the NDB scheme requirements, and include the following information:

- the identity and contact details of the Company.
- a description of the eligible data breach that the Company has reasonable grounds to believe has happened.
- the kind or kinds of information concerned; and
- recommendations about the steps that individuals should take in response to the eligible data breach.

This statement must also form the basis of the notification to individuals. Depending on the circumstances the Company will either:

- notify all individuals to whom the relevant information relates – this method will apply if it is not practicable to separately identify persons who may specifically be affected by the breach; or
- notify affected individuals – where particular individuals who are at risk from the breach are able to be separated out; or
- if neither of the above are practicable, communicate the breach by publishing a statement on the Company website and otherwise by taking reasonable steps to publicise it.

Review- The Response Team will conduct an investigation into the cause or causes of the breach. When the factors that contributed to the breach have been identified, a strategy will be developed to implement any recommendations to strengthen data security. The review will be made available to the Senior Leadership Team.

6. Responsibilities

Any notifiable data breaches will be reported to the Senior Leadership Team together with the data breach response plan. The SLT may consider additional reporting of certain breaches to:

- the Company's financial services provider.
- Australian Cyber Security Centre.
- police or law enforcement bodies.
- State Privacy and Information Commissioners.
- professional associations and regulatory bodies.
- insurance providers.

The Business Unit Manager is responsible for oversight of this policy and procedure, including the regular review and testing of the data breach response plan.

It is the responsibility of all staff to notify the Company of any suspected data breaches.

Status and Details

Status	Current
Effective Date	1 October 2022
Review Date	15 October 2022
Approval Authority	Global Head of Enterprise Technology, Risk and Cyber Security
Approval Date	19 October 2022
Expiry Date	Not Applicable
Responsible Executive	Chief Technology Officer
Enquiries Contact	Enterprise Technology Team