Data Breach Response Plan & Policy

Mondus Capital Pty Ltd ACN 659 284 312

August 2024 (Updated October 2025)

Table of Contents

1. Introduction

Zeroo Home Loans is a trading name of Mondus Capital Pty Ltd ACN 659 284 312 (Mondus). Mondus and Zeroo Home Loans are committed to expeditiously managing and protecting personal information in accordance with the relevant legislative framework in the event that Mondus experiences a data breach or suspects that a data breach has occurred.

This Data Breach Response Plan & Policy (Plan & Policy) outlines the procedures for staff and key personnel for reporting and dealing with suspected or known data breaches.

2. Objectives

The objectives of this Plan & Policy are to:

- ensure timely and appropriate response to data breaches;
- comply with legal and regulatory obligations under the *Privacy Act 1988* (Cth)(Privacy Act), *Corporations Act 2001* (Cth), *Australian Securities and Investments Commission (ASIC) Act 2001* (Cth), and *National Consumer Credit Protection Act 2009* (Cth); and
- the extent possible, mitigate the impact of data breaches on affected individuals and Mondus.

3. Legislative Obligations

The Privacy Act requires that Mondus protect personal information it collects from its customers and holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. This requirement extends to situations where Mondus engages a third party to store personal information on its behalf.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) requires Mondus to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of an Eligible Data breach.

Mondus must give a notification if:

a) it has reasonable grounds to believe that an eligible data breach has happened; or
b) it is directed to do so by the Commissioner.

4. What is a Data Breach?

A data breach occurs when personal information (Eligible Data) held by Mondus (or any third party engaged by Mondus to hold or process Mondus' data) is:

a) lost;

b) accessed, modified or disclosed without authority; or

c) misused or interfered with.

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. Information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming reasonably identifiable as a result.

The data subject to the breach could be in any form, e.g. electronic form or hard copy. For example, a data breach might occur if:

a) an employee of Mondus loses a laptop or USB stick that contains personal information;

b) Mondus accidentally discloses personal information to the wrong person (e.g. an email is sent to the wrong person); or

c) Mondus computer systems containing personal information are hacked into by a third party.

The following table provides a summary of common cyber incidents, including a data breach, and the corresponding initial response activities.

Type	Initial response
Data breach: unauthorised access to sensitive or personally identifiable information.	Contain the data spill and alert the Data Breach Response Team as soon as possible. Investigate the cause of the data loss/spill. Mondus' I.T provider should be informed as a matter of priority.
Ransomware: a tool used to encrypt or lock victims' data until a ransom is paid.	Immediately remove the infected device(s) from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined. Mondus' I.T provider should be informed as a matter of priority.
Malware Infections: a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.	Immediately remove the infected device(s) from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined. Mondus' I.T provider should be informed as a matter of priority.
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: overwhelming a network with traffic that it cannot process, sometimes impacting network availability.	Request gateway services provider to identify the DoS/DDoS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and or increase capacity. Mondus' I.T provider should be informed as a matter of priority.

Phishing and Social Engineering: deceptive communications designed to elicit users' sensitive information e.g. network and business login credentials.	Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took, and whether any personal or sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorised access. Mondus' I.T provider should be informed as a matter of priority.

There are many methods of achieving unauthorised network access, which may result in cyber incidents, such as a data breach. Ensuring awareness of these potential methods of unauthorised access will support Mondus in identifying deficiencies or commonly targeted areas of its network. A summary of common methods of unauthorised access includes:

Type	Initial response
External or Removable Media	An attack executed from removable media or a peripheral device.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.
Web	An attack executed from a website or web-based application.
Email	An attack executed via an email message or attachment.
Impersonation	For example, a domain that is created to imitate Mondus' in an attempt to deceive victims (typically associated with phishing attacks).
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

The Data Breach Response Team will undertake a yearly audit of information and data threats which have occurred to the business. The outcome of each annual audit will be discussed with the Directors and Data Breach Response Team. The outcome of each audit will be addressed accordingly.

5. Detecting a Suspected Data Breach

There are many methods for detecting data breaches, amongst the use of software to prevent data breaches, Mondus utilises the following general detection methods:

a) reconciliation: comparing two sets of data and explaining variances;
b) benchmarking: comparing two sets of data that would normally exhibit similar characteristics, in order to highlight material variations;

c) data profiling: examination of a data set and the gathering of statistics and other relevant information for the purposes of analysis to highlight any data anomalies (e.g. missing data, outliers, unexpected variances); and
d) a review of data for reasonableness using expert judgment.

6. Roles and Responsibilities

General Staff

General staff have the following responsibilities:

a) complying with the terms of this Policy & Plan and all other relevant Mondus policies, procedures, regulations and applicable legislation;
b) reporting actual, suspected, threatened or potential data breaches immediately to the Data Breach Response Team and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage;
c) not disclosing information to anyone, within or outside of Mondus, other than the Data Breach Response Team, until they are authorised by the same;
d) respecting and protecting the privacy and confidentiality of the information they process at all times; and
e) reporting all misuse and breaches of this Policy & Plan.

Data Breach Response Team

The Data Breach Response Team (DBRT) is responsible for overseeing all aspects of Mondus' response to the data breach in accordance with the Data Breach Response Plan. The team shall consist of the Chief Executive Officer, Chief Information Officer, Compliance Officer, and Legal Counsel (if applicable).

The DBRT must work through this Data Breach Management Plan to decide what steps that Mondus will take to manage and respond to the data breach or suspected data breach, then ensure those steps are taken.

The Compliance Officer has the following responsibilities:

a) ensuring this Policy & Plan is reviewed at least annually;
b) ensuring that implementation and compliance with this Policy & Plan is monitored/audited on a regular basis;
c) ensuring that this Policy & Plan and related policies, guidelines and procedures are accessible and communicated on a recurring basis;
d) overseeing management of any breach in accordance with the Data Breach Management Plan; and
e) reporting to the DBRT on compliance and relevant issues or considerations relating to the protection of eligible data from unauthorised use or accidental modification, loss or release.

The Compliance Officer has the following responsibilities:

a) providing an initial assessment which determines whether a data breach might have occurred;
b) determining whether a data breach is serious enough to escalate to the DBRT; and
c) reporting to the DBRT where a data breach is deemed serious enough.

7. Data Breach Response Plan

Step 1: Identification and Notification

- Immediate Action: Any employee who reasonably suspects that a data breach may, has or is likely to have taken place must notify the Compliance Officer immediately. The words "Privileged and Confidential" are to be in the subject or heading of any communications in relation to the suspected data breach. The employee should record and advise the Compliance Officer of:
    - the time and date the suspected breach was discovered;
    - the system(s) and hardware, if any, affected;
    - the type of information involved (i.e. personal information or confidential information);
    - a description of the information involved;
    - the cause and extent of the breach; and
    - the context of the affected information and the breach.

If an employee thinks the breach may require urgent action, they must report it immediately no matter what time of the day or night it is. It is better to err on the side of caution and report the matter to the Compliance Officer as soon as possible. Sometimes the full impact of a data breach is not immediately apparent.

- Acknowledgment: The Compliance Officer will acknowledge receipt of the report within 24 hours.

Step 2: Documentation, Assessment, and Containment

- Containment: If a data breach has or may have occurred, the Compliance Officer and Mondus' I.T provider will take immediate steps, to the extent that is possible, to contain the breach and prevent further unauthorised access and compromise of personal information. Care must be taken to not 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.

  If Mondus' I.T provider considers that the data breach can be quickly and easily contained with low risk of harm to any individual or to Mondus' reputation or business operations, Mondus' I.T provider should manage the incident and need not convene the Data Breach Response Team. In such a case the Mondus' I.T provider must:

    - initiate the steps required to contain the breach;
    - manage any further response to the breach that the Mondus I.T provider considers appropriate, such as:
        - discussing the matter with relevant employees;
        - suggesting any changes that may reduce the risk of a similar breach happening again; and
    - no further action under this Data Breach Management Plan (other than as outlined above) is required.

  Otherwise, the Technical Lead must convene the DBRT as soon as possible by contacting each member of the DBRT. The Technical Lead must brief the DBRT about the data breach.

  Once the DBRT has been convened and briefed by Technical Lead, it will be responsible for overseeing all aspects of AL&M'S response to the data breach including all further steps in this Data Breach Management Plan.

  All steps outlined in the checklist in Appendix I will be overseen by the DBRT.

- Documentation: The Compliance Officer will work with the employee in relation to the suspected data breach to gather documentation regarding the incident, including (but not limited to):
    - when the breach occurred;
    - when it was discovered;
    - which system(s) and hardware, if any, are affected
    - who discovered the breach and who subsequently accessed the affected system;
    - all persons aware of the breach;
    - the type(s) of data lost;
    - the risks of potential harm;
    - the existing training programs, security measures, procedures, protocols, policies, audit trails relevant to the breach and safeguards in place at the time of the incident occurring;
    - the extent of knowledge about the breach inside and outside of Mondus; and
    - any representations made to the relevant data subjects about how personal information they provided would be used and protected.

- Assessment: The Compliance Officer will conduct a preliminary assessment to determine whether a data breach has or may have occurred including (but not limited to):
    - the type of personal or confidential commercial information involved;
    - all persons aware of the breach;
    - who discovered the breach and who subsequently accessed the affected system;
    - the cause and extent of the suspected or potential breach; and
    - if there is or may be a real risk of serious harm to the affected individuals or Mondus' customers or other "business partners" now or in the future.

The Compliance Officer must document all evidence-based decisions and should consider whether remedial action can be taken to reduce potential harm to individuals at the Documentation, Assessment, and Containment step.

Step 3: Risk Evaluation

There is no single way to respond to a data breach. Each breach will need to be assessed on a case by case basis. It is important to understand the risks posed by each breach and the actions that would be most effective in reducing/removing the risks.

This is to be conducted in refence to the Serious Harm Test. This test considers whether the breach is likely to result in serious harm to any affected individuals now or in the future. A broad range of potential harms that may follow the data breach are to be considered by the DBRT.

Examples of scenarios resulting in serious harm may 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; or
- workplace or social bullying or marginalisation.

If the breach is likely to cause serious harm, proceed to the notification step.

The DBRT may determine its own working procedures. The DBRT may delegate work and decision-making powers internally within Mondus, and may engage external assistance, such as an external forensic expert, as it considers appropriate.

Before entering into any forensic investigation, Mondus should consider whether the investigation is for the purpose of establishing its legal position. If so, Mondus should consider retaining an external Legal Counsel in order to better support any future claim for legal professional privilege.

Step 4: Notification

If the data breach discloses personal information and a reasonable person would conclude that the data breach is likely to result in serious harm to any affected individual, Mondus is legally required to notify the individual of the breach (or if the data was being held by Mondus for a third party such as a client, Mondus should work with that third party to notify the individual).

If Mondus has reasonable grounds to suspect that a notifiable data breach may or is likely to have taken place, but is not certain, Mondus must quickly (and within no more than 30 calendar days) assess whether a notifiable data breach has occurred and report the breach to the OAIC accordingly.

An exemption to mandatory notification may apply in limited circumstances, if Mondus is:

a) able to take remedial action to ensure the data breach is not likely to result in serious harm to any individual; or
b) exempted by the Commonwealth Information Commissioner.

Australian Information Commissioner

Under the Privacy Act, Mondus is legally required to notify the OAIC about breaches that are likely to cause serious harm now or in the future that Mondus is unable to prevent the likely risk of serious harm with remedial action. This can be done by using the prescribed Notifiable Data Breach Form accessible on the OAIC website (https://webform.oaic.gov.au/prod?entitytype=DBN&layoutcode=DataBreachWF).

Affected Individuals

No communications must be made to affected individuals without the direct approval from DBRT.

If the DBRT determine that a notification is required, it will notify the affected individuals directly and as soon as practicable, providing them with:

- the identity and contact details of Mondus;
- a description of the breach;
- the type of information involved; and
- recommended steps they should take to mitigate potential harm.

In the event that urgent notification is required, notification must be done by phone or, if the affected individuals cannot be reached by phone, by email. A follow-up hard copy letter must be sent.

If it is not practical for Mondus to notify each affected individual directly (e.g. Mondus cannot find their current contact details or cannot determine who has been affected) and Mondus is required by law to notify them, Mondus must as soon as possible publish a statement about the data breach on its website and take reasonable steps to publicise the statement.

Other Parties

The DBRT must consider who else other than the affected individuals (and the Commissioner if the notification obligations of the Notifiable Data Breach scheme apply) should be notified.

At a minimum, Mondus will notify the following:

a) the media and the general public, e.g. through a media release, social media platforms and/or Mondus' website – but if a police force or another regulatory body is investigating, consult with them before making the breach public;
b) Mondus' clients or other "business partners"; and
c) Mondus' insurers.

Step 5: Review and Improvement

- Post-Incident Review: Conduct a thorough review of the incident to identify lessons learned and areas for improvement.
- Policy Update: The DBRT will make recommendations to the Senior Management Team to change policies and procedures accordingly to avoiding similar incidents in the future.

If appropriate, the DBRT will discuss the implications of the incident and the importance of privacy and data security with affected employees and contractors and consider implementing new training sessions, ongoing training and awareness-raising initiatives. Any failure to abide by Mondus' policies should lead to appropriate discipline.

The DBRT shall also re-evaluate third-party relationships and take appropriate action such as, but not limited to, making contractual changes, improvements in security measures and moving to a different vendor.

8. Compliance and Reporting

Mondus will ensure ongoing compliance with the Notifiable Data Breach Scheme and other relevant legislation. Regular training will be provided to general staff on data breach prevention and response.

9. Continuous Improvement

We will regularly analyse data breach incidents and feedback to refine our response process and enhance staff training on regulatory requirements and customer care best practices.

10. Contact Information

Data Breach Response Team

For all matters relating to privacy and breaches of privacy, please contact the Data Breach Response Team at contact@mymondus.com or 0422362290

Other contact details

Privacy regulators	
Office of the Australian Information Commissioner	Telephone: 1300 363 992 Post: GPO Box 5288, Sydney NSW 2001 Email: enquiries@oaic.gov.au Website: http://www.oaic.gov.au/
Spam Act regulator	
Australian Communications and Media Authority	Telephone: 1300 850 115 Post: PO Box Q500, Queen Victoria Building NSW 1230 Email: info@acma.gov.au Website: http://www.acma.gov.au/
Government cyber-crime and cyber-security agencies	
Australian Signals Directorate's Australian Cyber Security Centre (the national online system for reporting cyber-crime – will forward report to federal, state, local, or international law enforcement or regulatory agencies with jurisdiction)	Only accepts reports via website: https://www.cyber.gov.au/report-and-recover/report
Financial complaints authority	
Australia Financial Complaints Authority	Telephone: 1800 931 678 Post: GPO Box 3, Melbourne, VIC 3001 Email: info@afca.org.au Website: https://www.afca.org.au/make-a-complaint

11. Approval

This policy has been approved by the Senior Management of Mondus Capital Pty Ltd on 24th September 2024.

This document provides a comprehensive framework for responding to data breaches, ensuring compliance with relevant legislation and protecting the interests of both Mondus Capital Pty Ltd and affected individuals.

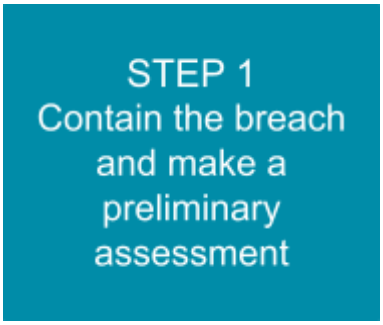
—---------

Zeroo Home Loans is a trading name of Mondus Capital Pty Ltd (ACN 659 284 312) and does not constitute a separate legal entity.

APPENDIX I

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 use that risk assessment to decide the appropriate course of action.

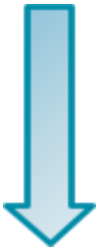
There are four key steps to consider when responding to a breach or suspected breach.



•	Convene a meeting of the DBRT and consider: • How did the 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 or harm to affected individuals?
•	Immediately contain breach: • IT to implement incident response plan if necessary. • Building security to be alerted if necessary.
•	IT to provide ongoing updates on key developments to DBRT.
•	Ensure evidence is preserved that may be

	valuable in determining the cause of the breach, or allow Mondus to take appropriate corrective action.
•	Consider developing a communications or media strategy to manage public expectations and media interest.

STEP 2
Evaluate 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 • how the breach was discovered and by whom • a list of the affected individuals, or possible affected individuals
•	What type of information is involved? The following types of personal information may involve high risk of harm to affected individuals: • health, genetic or biometric information • other "sensitive information" as defined in the *Privacy Act 1988* (Cth) e.g. political views, religious views, criminal record, racial or ethnic origin, membership of a trade association. • government identifiers, e.g. tax file numbers or Medicare numbers • bank account or credit card numbers • key identifying information about an individual that will never or rarely change, e.g. date of birth or residential address
•	Establish the cause and extent of the breach. • How much information is affected? • Which of the Mondus' customers are affected? • Is there a risk the breach will be repeated? • Is there evidence of

	theft/hacking/misconduct?
•	Assess priorities and risks based on what is known: • Was the information encrypted? How strong is the encryption? • Who has, or may have, gained access to the information? • How could the information be used? Could it be used for fraud or embarrassment?
•	Assess what harm could affected individuals, customers or "business partners" suffer? The risk may be higher or lower depending on who has received the information.
•	Assess what harm could Mondus suffer? • reputational damage (should the DBRT monitor any media, including social media, coverage of the data breach?) • damage to relationships with Mondus' customers or other "business partners" • loss of business • liability for breach of contractual, common law or statutory obligations of confidentiality/security/privacy (e.g. obligations owed to customers or other "business partners") • risk of regulatory penalties, e.g. for breach of the *Privacy Act 1988* (Cth)
•	What internal and/or external resources will be required to manage the consequences of this breach, e.g.: • does Mondus need to apply additional resources to monitor and respond to comments on social media sites? • does Mondus need external legal, public relations or crisis management

	advice?
•	Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decision made.

STEP 3
Consider the breach notification

•	Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
•	Determine whether to notify individuals – is there a *real risk of serious harm to the affected individuals?* 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 to affected individuals.
•	Consider whether others should be notified, including policy/law enforcement, or other agencies or organisations affected by the breach, or where the Mondus is contractually required or similar obligation to notify specific parties.

STEP 4
Review the incident and take action to prevent breaches

•	Fully investigate the cause of the breach.
•	Report to Senior Management on outcomes and recommendations: • Update security and response plan if necessary.

	• Make appropriate changes to policies and procedures if necessary. • Revise staff training practice if necessary. • Consider the option of an audit to ensure necessary outcomes are effected.