Privacy

Purpose

This Privacy Policy sets out our information handling policies. We are bound by the Australian Privacy Principles (**APPs**) and the Notifiable Data Breaches (**NDB**) scheme under the Privacy Act.

This policy explains how we will collect, store, verify, use and disclose this information we hold and the conditions under which information may be accessed. It also explains our obligations for responding to data breaches.

Our privacy policy contained on our website (**Privacy Policy**) is also set out in this policy.

PROCEDURES – THE REPORTING OFFICER MUST ENSURE THAT:	
1	The provisions of the Privacy Policy are reviewed annually to reflect any changes to our processes and systems in relation to how we handle personal information.
2	The contact details for the Licensee are updated if changes occur.
3	Data breach incident response, assessment and notification obligations are followed.
4	Training on the Privacy Policy and responding to data breaches is carried out in accordance with the training policy.

Privacy

We are bound by the Privacy Act and any amendments including the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), and the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), and we will protect your personal information in accordance with the Australian Privacy Principles (**APPs**). These principles govern how we can collect, use, hold and disclose your personal information, and how we respond when a data breach (including cyber and data security breaches) is likely to result in serious harm to any individuals whose personal information is involved in the breach.

Privacy Policy

We are committed to protecting your privacy and complying with Australian Privacy Principles under the *Privacy Act 1998* (Cth) (the Privacy Act). As part of our commitment and to explain how we collect, manage and handle your personal and/or sensitive information, we have developed our Privacy Policy.

What kinds of personal information do we collect and hold?

When you apply for an interest in any of our funds (**Funds**), we may collect information that is necessary to be able to provide you with an interest in a Fund. For instance, we may ask for identification information such as your name, address, and date of birth. Any unsolicited personal information we may collect will be promptly destroyed.

We may also collect other information as may be required from time to time either to provide financial products and services to you or ensure compliance with the law.

Why do we collect, hold, use and disclose personal information?

The main reason we collect, use, hold and disclose personal information is so we can service your request concerning a Fund. This may include:

- checking your eligibility for a Fund;
- providing you with a Fund; and
- helping you manage your interests in a Fund.

How do we collect personal information?

We collect most personal information directly from you. Sometimes we collect personal information about you from other people such as publicly available sources of information.

Some of our products and services are offered by intermediaries such as financial planners, solicitors and/or accountants and we may collect personal information about you from these third parties, if and where applicable.

How do we hold personal information?

Much of the personal information we hold will be stored electronically and securely by us at the offices of a Fund administrator. We use a range of security measures to protect the personal information we hold.

Who do we disclose your personal information to and why?

Sometimes we may disclose your personal information to organisations outside the Licensee. For example, with the administrator of a Fund, so that it may perform its duties for a Fund and our services.

What is an eligible data breach?

In accordance with the NDB scheme of the Privacy Act, we (along with our service providers) will notify you of any unauthorised access, disclosure or loss of personal information.

In these circumstances, we perform an assessment to determine if there has been an 'eligible data breach'. To do so, we consider if the access or disclosure of personal information is *likely to result in serious harm* to the individuals affected by the suspected data breach.

If we determine there has been an 'eligible data breach', then you will be notified as soon as practicable. We will notify you with the details of the breach and the recommended steps to take to mitigate any concerns. As required, we will report an 'eligible data breach' to the Office of the Australian Information Commissioner (**OAIC**).

In summary, subject to certain exemptions, the NDB scheme requires us to:

- carry out a reasonable and expeditious assessment if there are reasonable grounds to suspect that there may have been an eligible data breach (and to take reasonable steps to complete that assessment within 30 days); and
- make the prescribed notifications (to OAIC, and if practicable, to affected individuals) as soon as we are aware that there are reasonable grounds to believe that there has been an eligible data breach. The notifications must include a description of the data breach, the kinds of information concerned and recommendations about the steps individuals should take in response to the data breach.

Who do we notify when there is a data breach of your personal information?

We are obliged to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm (i.e. 'eligible data breaches'). This notification must include recommendations about the steps individuals should take in response to the breach. The OAIC must also be notified of eligible data breaches.

Do we disclose personal information overseas?

We may disclose your personal information to recipients located outside Australia. These entities may include our service providers, which perform technology, operational and customer service functions on our behalf and may have hosting and cloud service providers in locations outside of Australia.

We will only do so in compliance with all applicable Australian data protection and privacy laws. We will not disclose your personal information to an overseas recipient unless we have taken reasonable steps to ensure that the recipient protects your privacy according to the Australian Privacy Principles. Nor will we sell your personal information or otherwise disclose it to a third party for a purpose which unrelated to a product or service we are providing to you.

We have a strict duty to maintain the privacy of all personal information we hold about you, however certain exceptions may apply. For example, disclosure of your personal information may be authorised or required:

- By law (e.g. disclosure to courts under subpoena or to various government departments and agencies such as the Australian Taxation Office).
- In the public interest (e.g. where a crime, fraud or misdemeanour may be committed or suspected or with your consent, your consent may be implied or express and it may also be verbal or written).

Do we use or disclose personal information for marketing?

We may use your personal information to offer you other products and services that we believe may interest you. We will not do this if you tell us not to.

If you don't want to receive marketing offers from us, please contact us on the details listed at 'Contact us' below.

Access to and correction of personal information

You can request access to the personal information we hold about you. You can also ask for corrections to be made on information that you may believe is inaccurate, incomplete or out of date.

To request access or to make any corrections, please contact us on the details listed at 'Contact us'.

Resolving your privacy concerns and complaints - your rights

We will endeavour to respond to any privacy complaints within 30 days.

If you are not satisfied with our response to your privacy complaint, you may seek a review by contacting the OAIC:

Website: www.oaic.gov.au/contact-us

Phone: 1800 363 992

Email: enquiries@oaic.gov.au

Mail: Office of the Australian Information Commissioner

GPO Box 5288

Sydney NSW 2001

Contact us

If there is anything you would like to discuss, please contact us. If you have any questions or concerns about our privacy policy or practices, please contact us using one of the following methods:

- Email – info@coronetinvestments.com.au
- Website contact form – www.coronetinvestments.com.au/contact-us
- Phone – +61 414 209 227

This information is provided for information only. It does not constitute an offer or invitation to enter into any legal agreement of any kind for financial products or services.

Operations Procedure

This is the operations procedure we follow to maintain a Data Breach Response Plan and what actions to take if we suspect there is a data breach.

Depending on the size of the Licensee, a dedicated response team may be established to implement the Data Breach Response Plan. In any case, staff are appointed to adhere with our Data Breach Response Plan.

Data Breach Response Plan

What is a Data Breach?

A data breach occurs when personal information that we hold is subject to unauthorised access or disclosure or is lost. The likely risk of serious harm cause by a suspected data breach must also be considered. Serious harm can include:

- identity theft, which can affect your finances and credit report
- financial loss through fraud
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual's reputation.

If a data breach is likely to cause serious harm, it is considered an 'eligible data breach' and we are required to notify the OAIC via its online portal (see link below).

Containing, assessing and managing data breaches

We set out the actions our staff take in the event of a data breach or a suspected data breach. We must consider the capabilities of our staff to adequately assess data breaches and their impact.

In the event of a data breach, we implement a clear and immediate communications strategy that allows for the prompt notification of affected individuals and other relevant entities. In particular:

- who is responsible for implementing the communications strategy
- determining when affected individuals must be notified
- how affected individuals will be contacted and managed
- criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media); and
- who is responsible for liaising with external stakeholders.

The roles and responsibilities of staff

We expressly advise:

- who staff should inform immediately if they suspect a data breach; and
- the circumstances in which a manager can handle a data breach, and when a data breach must be escalated to the response team, if required.

The following factors may determine when a data breach is escalated to the response team, as required:

- the number of people affected by the breach or suspected breach
- whether there is a risk of serious harm to affected individuals now or in the future
- whether the data breach or suspected data breach may indicate a systemic problem with our practices or procedures; and
- other issues relevant to our circumstances, such as the value of the data to us or issues of reputational risk.

Documentation

We consider how our entity will record data breach incidents, including those that are not escalated to the response team as required.

Advice to provide to the affected party

In the event of a data breach, below is some suggested advice to provide the affected party.

- To report the cybercrime - the Australian Cyber Security Portal:
    - Online portal – https://www.cyber.gov.au/report-and-recover/report
    - Phone – (Australia) 1300 292 371
- To manage your compromised personal information - IDCARE:
    - Online – https://www.idcare.org/contact/get-help
    - Phone – (Australia) 1800 595 160, (New Zealand) 0800 121 068

Below are some other entities to contact:

Your bank

Bank	**Phone**
ANZ	1800 033 844
Commonwealth Bank	13 2221
National Australia Bank	1800 033 103
St George	1800 028 208
Westpac	1300 651 089
BankWest	1300 368 748

Credit rating agencies (**CRAs**) – to apply for a credit ban

- You can apply for bans with all the Australian CRAs by engaging just one credit reporting agency and requesting that they place bans with all CRAs if you agree to their terms and conditions.

Credit reporting agency	**Online form**
Equifax	www.equifax.com.au/eform/submit/credit-ban
illion	www.illion.com.au/credit-report-ban-request/
Experian	https://experian-apac-acb.my.site.com/banrequest/s/ban-request-form

Review

When evaluating how a data breach occurred, and the success of our response, we consider:

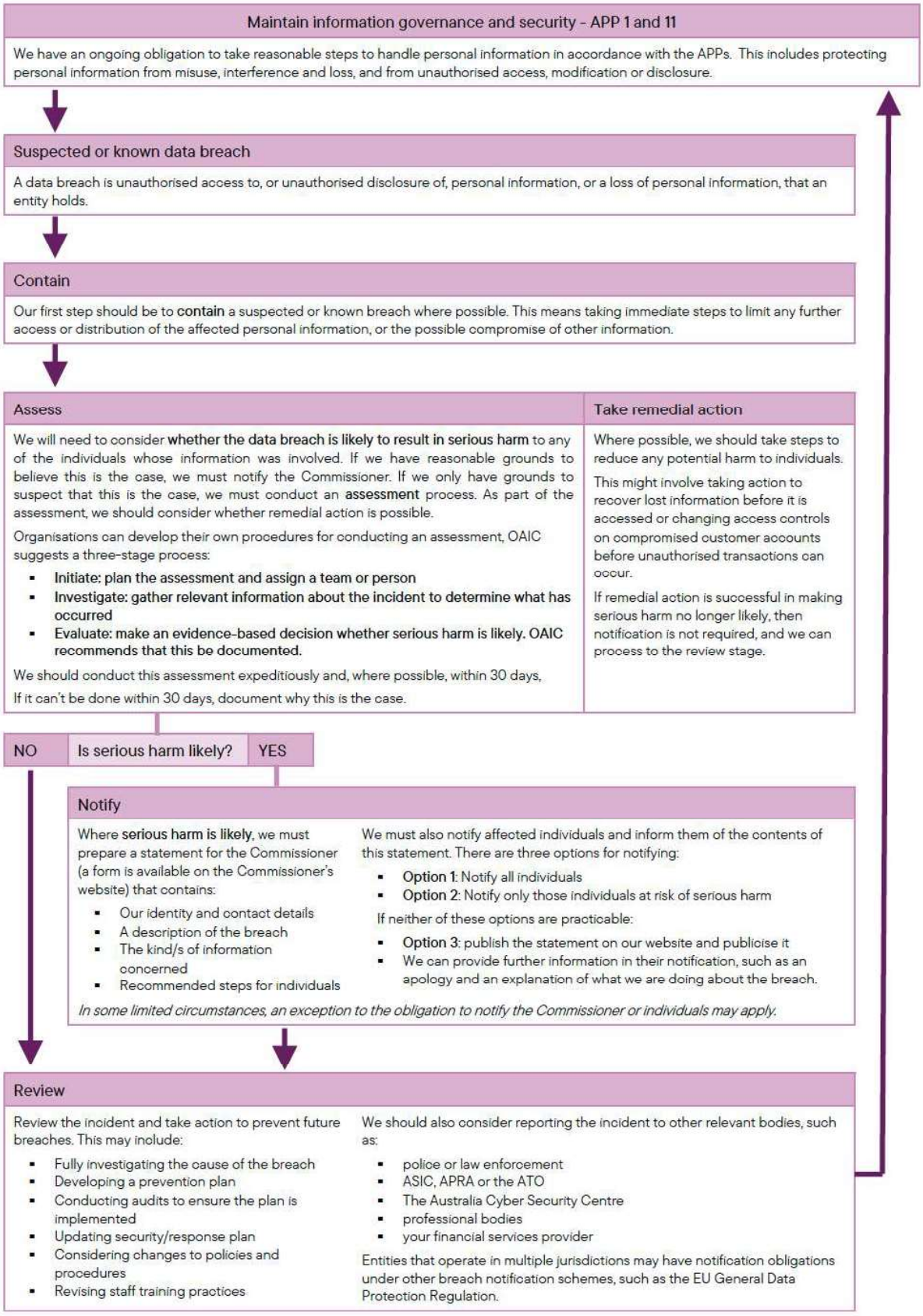
- a strategy to identify and address any weaknesses in data handling that contributed to the breach
- a system for a post-breach assessment of our entity's response to the data breach and the effectiveness of your data breach response plan.

If an eligible data breach occurs within our organisation, we notify the OAIC using the **below** link:

https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion

Operations Procedure

This is the operations procedure to follow if you suspect there is a data breach.



Step 1: Contain

Once you have discovered or suspect that a data breach has occurred, you should immediately take action 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 the physical or electronic security.

Addressing the following questions may help you identify strategies to contain a data breach:

- 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 of harm to affect individuals?

At this point, you may suspect an eligible data breach under the NDB scheme has occurred, which would trigger an assessment obligation. Or you may believe the data breach is an eligible data breach, which requires you to notify individuals as soon as practicable.

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would not enable you to address all risks potentially posed to affected individuals or entities.

Step 2: Assess

An assessment of the data breach can help you understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, you can ensure you understand the risk of harm affected individuals, and allow you to identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist entities in deciding whether affected individuals must be notified.

In your assessment of a data breach, consider:

- The type or types of personal information involved in the data breach.
- The circumstances of the data breach, including its cause and extent.
- The nature of the harm to affected individuals, and if this harm can be removed through remedial action.

All entities should consider whether remedial action can be taken to reduce any potential harm to individuals. This might also take place during Step 1: Contain, by recovering lost information before it is accessed.

Entities subject to the NDB scheme are required to conduct an assessment of 'suspected' eligible data breaches and take reasonable steps to complete this assessment within 30 days.

Step 3: Notify

Notification can be an important mitigation strategy as it has the potential to benefit both you and the individuals affected by the data breach. The challenge is to determine when notification is appropriate. Sometimes, 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 a breach notification is required.

Consider:

- Your obligations under the NDB scheme. You are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm.
- Whether another entity has fulfilled your notification obligations under the NDB scheme such as entity that holds client information on your behalf.

- Other circumstances in which individuals should be notified. For example, you may not have obligations under the NDB scheme, but have processes in place to notify individuals in certain circumstances.
    - What information is provided in the notification.
    - How the notification will be provided to individuals.
    - Who is responsible for notifying individuals and creating the notification.
- Who else other than affected individuals (and the Commissioner 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.
- Where the incident triggers reporting obligations to or for other entities.

An effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of your organisation or agency. 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 changing account passwords or being alert to possible scams resulting from the breach. It is important that staff are capable of engaging with individuals who have been affected by a data breach with sensitivity and compassion, in order to not exacerbate or cause further harm. Notification can also help build trust in an entity, by demonstrating that privacy protection is taken seriously.

Step 4: Review

Once steps 1 to 3 have been completed, you should review and learn from the data breach incident to improve your professional 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 the 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 employee selection and training practices.
- A review of service delivery partners that were involved in the breach.

In reviewing the information management and data breach responses you can refer to the OAIC's Guide to Securing Personal Information.

When reviewing a data breach incident, it is important to use the lessons learned to strengthen the entity's personal information security and handling practices, and to reduce the change 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 polices or procedures.

If any updates are made following a review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.