Privacy Policy

Purpose

This privacy policy sets out our information handling policies.

We are bound by the Australian Privacy Principles 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 in our website (**Privacy Policy**) is also set out in this policy on page 34.

PROCEDURES – THE REPORTING OFFICER MUST ENSURE THAT:	
1	The provisions of the Privacy Policy are reviewed semi-annually (March and September) 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, the Amendment (Enhancing Privacy Protection) Act, and the Privacy Amendment (Notifiable Data Breaches) Act. We will protect your personal information in accordance with the Australian Privacy Principles (**APP**s). 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.

The below Privacy Policy applies to any stakeholders we engage from time to time, and is included on our website homepage with the title 'Privacy Policy'.

Privacy Policy

What kinds of personal information do we collect and hold?

When you use, apply for, or speak to us about our provision of financial services to you (for example, financial advice or applying for an interest in a fund), we may collect information that is necessary to be able to provide you with financial services. 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.

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 for financial services. This may include:

- Checking your eligibility for our financial services;
- Providing you with financial services; and
- Helping you manage our financial services.

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.

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 the 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 the fund and our financial services.

What is an eligible data breach?

In accordance with the Scheme of the Privacy Act, we (along with our service providers) are required to 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 the affected party will the details of the breach and the recommended steps to take to mitigate any concern. 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 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 the 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?

The Notifiable Data Breaches (**NDB**) scheme under the Privacy Act requires us to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm (these are referred to as 'eligible data breaches'). This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (**Commissioner**) must also be notified of eligible data breaches.

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 the Commissioner, 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.

Do we disclose personal information overseas?

We may disclose your personal information to recipients located outside Australia. These entities may include our service providers.

Do we use or disclose personal information for marketing?

We may use your personal information to offer you further financial 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. To do so, please contact us on the details listed at 'Contact us' (below).

Resolving your privacy concerns and complaints – your rights

If you are concerned about how your personal information is being handled or if you would like to make a complaint, please contact us on the details listed at 'Contact us' (below).

If you are not satisfied by our response to an error or complaint about our privacy practices, you may refer to the OAIC (see www.oaic.gov.au).

If you are unhappy with our response, there are other bodies you can go to.

Office of the Information Commissioner
PO Box 10143
Adelaide Street Brisbane
Queensland 4000
Telephone: (07) 3234 7373 or 1800 642 753
Web: https://www.oic.qld.gov.au

Australian Financial Complaints Authority

GPO Box 3
Melbourne, VIC 3001
Telephone: 1800 931 678
Web: https://www.afca.org.au

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 – contact@nucleuswealth.com
- Website contact form – nucleuswealth.com
- Phone – 1300 623 863

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

Operations Procedure – Data Breach Response Plan

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

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

Data Breach Response Plan

What is a Data Breach?

A data breach occurs when personal information that you 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 you are required to notify the OAIC via their online portal (see link **below**).

Containing, assessing and managing data breaches

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

In the event of a data breach, you 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)
- who is responsible for liaising with external stakeholders

The roles and responsibilities of staff

You expressly advise:

- who staff should inform immediately if they suspect a data breach
- 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 your 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

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

Review

When evaluating how a data breach occurred, and the success of your response, you should 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 your organisation, you must notify the OAIC using the **below** link:

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

Operations Procedure – Managing Data Breaches

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

Maintain information governance and security - APP 1 and 11

We have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, that an entity holds.

Contain

Our first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

We will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If we have reasonable grounds to believe this is the case, we must notify the Commissioner. If we only have grounds to suspect that this is the case, we must conduct an **assessment** process. As part of the assessment, we should consider whether remedial action is possible.

Organisations can develop their own procedures for conducting an assessment, OAIC suggests a three-stage process:

- **Initiate: plan the assessment and assign a team or person**
- **Investigate: gather relevant information about the incident to determine what has occurred**
- **Evaluate: make an evidence-based decision whether serious harm is likely. OAIC recommends that this be documented.**

We should conduct this assessment expeditiously and, where possible, within 30 days.If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, we should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required, and we can process to the review stage.

NO | **Is serious harm likely?** | **YES**

Notify

Where **serious harm is likely**, we must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- Our identity and contact details
- A description of the breach

We must also notify affected individuals and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- Option 2: Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3**: publish the statement on our website and publicise it

- The kind/s of information concerned
- Recommended steps for individuals

- We can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review	
Review the incident and take action to prevent future breaches. This may include: • Fully investigating the cause of the breach • Developing a prevention plan • Conducting audits to ensure the plan is implemented • Updating security/response plan • Considering changes to policies and procedures • Revising staff training practices	We should also consider reporting the incident to other relevant bodies, such as: • police or law enforcement • ASIC, APRA or the ATO • The Australia Cyber Security Centre • professional bodies • your financial services provider Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.