COMPLIANCE INCIDENT AND BREACH REPORTING POLICY

Introduction

The aim of this Policy is to target breaches are properly identified, assessed, rectified, and reported on in a timely manner.

Legislative and Regulatory Requirements

AFSL Obligations

As an Australian Financial Services Licence ('AFSL') holder, the Company is subject to the breach reporting requirements under s912D of the Corporations Act 2001 ('the Act').

Pursuant to s912D of the Act, the Company has a legal duty to report actual or likely significant breaches or breaches of any of the specified obligations to ASIC within 10 business days of becoming aware of the actual or likely breach.

The below table summarises the specified obligations applicable to the Company.

Obligations under s912A and 912B	**Obligations under s912A(1)(c)**
The Company must: • do all things necessary to target that the financial services covered by its licence are supplied efficiently, honestly and fairly; • comply with the conditions of its licence; • have adequate resources to provide the financial services covered by its licence and to carry out supervisory arrangements; • be competent to supply the financial services covered by its licence; • have trained and competent representatives; • take reasonable steps to target that its representatives comply with the financial services laws; • have a dispute resolution system for retail clients; • have adequate risk management systems; and • have compensation arrangements for retail clients.	The Company must comply with the following financial services laws: • Ch 5C of the Act (managed investment schemes); • Ch 6C of the Act (information about ownership of listed companies and managed investment schemes); • Ch 7 of the Act (financial services and markets) • Ch 9 of the Act (miscellaneous), but only as it applies to the chapters of the Corporations Act listed above; • Div 2 of Pt 2 of the ASIC Act (unconscionable conduct and consumer protections for financial services); and • other Commonwealth Acts specified in reg 7.6.02A (see note below) in so far as they cover conduct when supplying financial services. [2]

Note: The Commonwealth Acts specified in reg 7.6.02A are the Banking Act 1959, Financial Sector (Collection of Data) Act 2001, Financial Sector (Shareholdings) Act 1998, Financial Sector (Transfer of Business) Act 1999, Insurance Acquisitions and Takeovers Act 1991, Insurance Act 1973, Insurance Contracts Act 1984, Life Insurance Act 1995, Retirement Savings Accounts Act

[2] *As at the date of this Policy, none of the Commonwealth Acts specified in reg 7.6.02A is applicable to the Company.*

1997, Superannuation Industry (Supervision) Act 1993 and Superannuation (Resolution of Complaints) Act 1993.

Responsible Entity Obligations

Pursuant to section 601FC(1)(l) of the Act, a responsible entity has a legal duty to report to ASIC any breach of the Act that relates to a registered managed investment scheme that has had, or is likely to have, a materially adverse effect on the interests of members of the scheme (i.e. the 'unitholders').

Breaches are required to be reported as soon as practicable after the responsible entity becomes aware of the breach.

Key Terms

- **Incident** – an error or adverse event that may be or lead to a breach.
- **Breach** – a breach includes, failure by the Company and/or its representatives to meet:
- AFSL obligations;
- Financial services laws;
- Scheme's constitution or compliance plan (for the responsible entity);
- Material service provider agreements;
- Internal policies and standards; and
- Disclosure documents.

Identification and Detection of Breaches

Breaches may be identified:

- Through complaints or incidents upon notification to the Chief Operating Officer (COO). The complaint or incident will be formally documented in the *"Pella Incident Report Template"* and recorded in the Incidents Register. From reviewing the report, the COO will determine whether the incident constitutes a breach. The COO will then investigate the incident/breach and advise the involved parties what the appropriate remedial action will be;
- By staff members who may come across a breach during their day-to-day duties where such a breach may have been caused either by their own conduct or by that of another staff member;
- By the COO when reviewing regulatory or AFSL obligations of the Company, or during the monitoring and reviewing of policies and procedures;
- By an external auditor of the unregistered or registered managed investment scheme; and
- By an external service provider.

Internal Reporting of Incidents

All incidents should be reported to the COO and/or the Director as soon as possible, to assess whether the incident may involve an actual or likely breach. The *"Pella Incident Report Template"* is included in the Appendix – Compliance Incident & Breach Reporting. The *"Report"* comprehensively documents the particulars of the incident, and the possible risk/impacts faced by Pella.

Timely reporting to the COO and/or Chief Operating Officer is critical, as depending on the nature of the breach, it may need to be escalated immediately and/or reported to ASIC.

The COO records all actual or likely breaches in the Incident Register.

Rectification Action

The COO will liaise with the relevant staff member to target that the cause of the breach is identified, and a rectification process is established and implemented.

Depending on the nature and extent of non-compliance, remedial action could include:

- Additional training;
- Additional monitoring or supervision;
- Formal reprimand;
- Notification to relevant regulatory body; and
- Termination of employment (in particularly serious cases).

In determining what remedial action will be appropriate, consideration should be given to the following matters:

- The number or frequency of similar previous instances of non-compliance by the officer, employee and/or agent (including our service providers);
- Whether the non-compliance was intentional or reckless;
- The impact the non-compliance has on the ability of the Company to continue to provide the financial services covered by its AFSL;
- The actual or potential loss arising to the Company or a client of the Company because of the non-compliance;
- Actions outlined in the Code of Conduct;
- Any other relevant facts associated with the non-compliance; and
- Any other relevant issues raised.

The COO has the authority to approve any remedial actions or rectification processes. However, the COO may refer the matter to a Director, Compliance Committee (for registered managed investment schemes) or the Board, if appropriate.

The COO is responsible for monitoring the rectification process to target that all actual or likely breaches are resolved as planned. The rectification action, including date of rectification, will be documented in the Breach Register.

Where an actual or likely breach evidences systemic issues, the COO is to target that internal procedures are reviewed and amended where necessary.

Assessment of Breaches

In considering whether a breach is significant under the test in s912D of the Act[3] the following matters will be considered:

- The number or frequency of similar previous breaches;
- The impact the breach has had or will have on the Company's ability to provide the financial services covered by its licence;
- The extent to which the breach or likely breach indicates that the compliance arrangements might be inadequate;

[3] *ASIC RG 78 Breach reporting by AFS licensees*

- The actual or potential loss to clients or to the Company itself, arising from the breach or likely breach; and
- Any other relevant matters including those prescribed by regulations.

Some examples of significant breaches may be:

- Breach of the financial requirements of an AFSL condition;
- A breach which causes actual or potential financial loss to a client or unitholder (unless it is isolated, involves a small number of clients/unitholders and the loss involved is immaterial);
- Failure to maintain the appropriate level of professional indemnity cover where required to do so;
- Failure to prepare cash flow projections;
- Identification of previously undetected breaches;
- Representatives acting outside the scope of the AFSL conditions; and
- Fraud in the provision of financial services by a representative.

Some examples of breaches which would not be considered significant may be:

- Isolated provision of inappropriate advice by representatives; and
- Unit pricing errors of an immaterial amount involving a small number of clients.

Where an actual or likely breach is considered to be significant by the COO, the incident would be immediately escalated to the Director and/or Board for consideration and reported to ASIC within the statutory timeframe.

The COO is responsible for reporting significant breaches to ASIC.

If the breach is not considered to be significant, the COO reports all actual or likely breaches to the Compliance Committee (for registered managed investment schemes) and the Board at their next meetings.

Reporting to ASIC

A breach or likely breach which is reported to ASIC will include at least the following information:

- The date of the breach or the date from which it is anticipated that the Company will no longer be able to comply with its obligations;
- The duration of the breach;
- The date when the COO first became aware of the breach;
- A description of the breach and how it was identified;
- A description of why the breach is significant and a description of the factors that have been considered;
- A description of the obligation/s that have been breached;
- Whether the breach has been rectified and/or the steps taken to remedy the breach; and
- Steps that have been taken to prevent a similar breach occurring.

Where an actual or likely breach is significant, a breach report must be given to ASIC in writing. Notifications can be provided on an ASIC Form FS80 – 'Notification by an AFS licensee of a significant breach of a licensee's obligations.

Completed breach report will be sent by the COO to ASIC either by mail to 'Misconduct and Breach Reporting, Australian Securities and Investment Commission' or email at fsr.breach.reporting@asic.gov.au.

Trading Breaches

A trading breach is defined as entering a breach that results in a position or the portfolio sitting outside of the stock or portfolio limits communicated to Pella's clients. Table 1 summarises these limits and the temporary tolerance level. The temporary tolerance level is established to allow for situations where the portfolio might temporarily contravene a limit. The portfolio/trading can contravene these limits for up to one week before they must be rectified.

Table 1 – Portfolio limits

Factor	Limit and rules	Temporary tolerance level
Number of stocks	30-50	0
Country	10% above the Benchmark weight and there is no minimum exposure	+2.5%
Region	25% above the benchmark, with no minimum	+2.5%
Sector	25% of the Fund	+2.5%
Maximum cash	20%	+2.5%
Liquidity	Liquidate 67% of the fund within five business days	
Target minimum market cap at initial investment	US1.5Bn	$100m
Segment		
Core	60-80% of portfolio	±2.5%
Cyclical	0-30% of portfolio	±2.5%
Innovation	0-20% of portfolio	±2.5%
ESG Ratings		
AAA, AA, A	>30% of the portfolio	±2.5%
AAA, AA, A, BBB	>70% of the portfolio	±2.5%
BB, B	< 30% of the portfolio	±2.5%
CCC	0% of portfolio	±2.5%
Excluded activities		
Alcohol manufacturing	0% with 0% revenue materiality	±2.5%
Animal cruelty	0% with 0% revenue materiality	±2.5%
Correctional facilities	0% with 0% revenue materiality	±2.5%
Deforestation	0% with 0% revenue materiality	±2.5%

Fossil fuel generation	0% revenue materiality for thermal coal and 20% revenue materiality for gas [1]	±2.5%
Fossil fuel mining or exploration	0% with 0% revenue materiality	±2.5%
Gambling	0% with 0% revenue materiality	±2.5%
GMO seeds manufacturing	0% with 0% revenue materiality	±2.5%
Norms-based	0% with 0% revenue materiality	±2.5%
Porn	0% with 0% revenue materiality	±2.5%
Uranium mining	0% with 0% revenue materiality	±2.5%
Weapons	0% with 0% revenue materiality	±2.5%

Monitoring Compliance with this Policy

The COO is responsible for monitoring compliance with this Policy. As part of the monitoring process, the COO will review matters such as the external audit reports and the Complaints Register to identify any instances of non-compliance. The Breach Register will be reviewed to identify any systemic issues.

Any instances of non-compliance by representatives of the Company will be reported to the Compliance Committee (if applicable) and the Board. Instances of non-compliance may also be treated as a potential or actual breach and dealt with according to this Policy.

Intentional or reckless non-compliance with this Policy is not tolerated by the Board.

If systemic non-compliance is the result of action by a service provider, then this is an event which shall be reported to the Board for their consideration. The Board will consider what additional monitoring and remedial action may be required which could include consideration as to whether the service agreement should be terminated.

Appendix – Compliance Incident & Breach Reporting

Incident Report

Email report to tony.hammond@pellafunds.com

Administration

Date occurred:
Date identified:
Date resolved:
Identified by:
Report prepared by:
Parties impacted:
Responsible Entity/Trustee:
Fund Manager:

Fund/Mandate:

Incidence details

Is this incident also a complaint? (Yes/No)
What happened?
How was it identified?
Number of investors affected
Dollar and/or bps impact
Cause of event
Resolution action
What has been implemented to target it does not happen again?

Regulatory assessment

What regulation or policy has been breached?
Is it reportable to ASIC? **If not, why not?**

Significant breach triggers:

- the number or frequency of similar previous breaches;
- the impact of the breach or likely breach on the licensee's ability to provide the financial services covered by the licence;
- the extent to which the breach or likely breach indicates that the licensee's compliance arrangements are inadequate; and
- the actual or potential financial loss to clients of the licensee arising from the breach or likely breach.

Pursuant to section 601FC(1)(l) of the Corporations Act, a Responsible Entity has a legal duty to report to ASIC any breach of the Act that relates to the Scheme and has had, or is likely to have, a materially adverse effect on the interests of members of the Scheme ('Unitholders').

Trading Breach Register

The Company is required to:

- Record all fund trading/portfolio breaches in the Trading Breach register.
- A breach is defined as any trade that will result in the portfolio falling outside of the limits illustrated in Table 2.

Table 2 – Trading Breach Register

No.	Stock code	Stock name	Date of breach	Description of breach	Explanation for breach	Date resolved
1				• The portfolio or stock limit that was breached e.g. min market cap size, exposure to banned activities, sector exposure	• Why the breach occurred	

Breach Register Template

The Company is required to:

- Record all breaches of Company's compliance systems and processes in this Breach Register
- Report all significant breaches to ASIC within 10 business days (and in some cases immediately)
- Report to ASIC any breach of the Act that relates to the registered managed investment scheme and has had, or is likely to have, a materially adverse effect on the interests of members/unitholders as soon as practicable after it becomes aware of the breach
- Report any breaches of financial requirements immediately to ASIC where required

Table 3 – Breach register template

No	Date Identified	Section / Procedure / Process Breached	Details of Breach	Assessment of significance of breach (s601FC and s912D) (COO to Complete)	Action Plan to Remedy Breach and Details of any Newly Implemented or Amended Controls	Completion Date for Each Action	Person Responsible for Breach Remedy	Date ASIC Notified
1.			• Date breach occurred and • Date breach was rectified • Entity/s to which the breach relates • Description of the breach • Description of what has been breached • Cause of the breach • Who identified the breach • How the breach was identified • Consequences of the breach.	In accordance with s601FC, it is not considered that this breach has had, or is likely to have, a materially adverse effect on the interests of clients or unitholders. This breach was not considered to be "significant" in accordance with s912D because: • The number or frequency of similar previous breaches; • The impact of the breach or likely breach on the licensee's ability to provide the financial services covered by the licence; • The extent to which the breach or likely breach indicates that the licensee's arrangements to target compliance with those obligations is inadequate; • The actual or potential financial loss to clients of the licensee, or the licensee itself, arising from the breach or likely breach				