



AIMS Funds Management
A Member of AIMS Financial Group

BREACH REPORTING POLICY

January 2016

TABLE OF CONTENTS

- 1. BREACHES3**
 - 1.1. BACKGROUND3
 - 1.2. OVERVIEW.....3
- 2. WHAT IS A “BREACH”?4**
 - 2.1. WHAT DOES “LIKELY TO BREACH” MEAN?4
- 3. RESPONSIBILITIES IN RELATION TO BREACHES5**
 - 3.1. WHEN IS A BREACH REQUIRED TO BE REPORTED TO ASIC?6
 - 3.2. WHAT IS A SIGNIFICANT BREACH?6
- 4. ACTION TO BE TAKEN FOLLOWING THE IDENTIFICATION OF A BREACH8**
 - 4.1. HOW ARE RECORDS OF BREACHES MAINTAINED?8
- 5. TRAINING9**

BREACHES

1.1. BACKGROUND

The AIMS Funds Management group (“**AIMS**”) has prepared this policy based on the requirements in ASIC Regulatory Guide 78 – Breach Reporting by AFS Licensees. AIMS Funds Management Group consists of AIMS Fund Management Limited, AIMS Real Estate Funds Limited and AIMS Investment Managers Limited.

This policy will be reviewed and approved by the Board at least annually. The Board will monitor all breaches and will ensure that adequate resources are allocated to the process.

The Compliance Officer will ensure that training on the breach reporting process is conducted for all employees at induction and on an ongoing basis.

1.2. OVERVIEW

The identification, management and reporting of breaches is important because, in addition to rectifying the particular breach:

- (a) It provides an opportunity to learn from mistakes and review and improve in the areas where the breach occurred; and
- (b) The Corporations Act requires that certain “significant” breaches and likely breaches of our obligations as a financial services licensee, including obligations to comply with the Corporations Act, are notified to ASIC in writing as soon as practicable, and in any case, within 10 business days of becoming aware of the breach.

All employees are expected to take a pro-active approach to the identification, management and reporting of all breaches that have occurred, or are likely to occur.

2. WHAT IS A “BREACH”?

A breach is broadly classified as a violation of, or failure to comply with, the Corporations Act, ASX Listing Rules, AFS Licence conditions, Fund Constitutions, Fund Compliance Plans or internal policies of AIMS. Section 912D(1B) of the Corporations Act states that a financial services licensee must, as soon as practicable and in any case within 10 business days after becoming aware of the breach or likely breach, lodge a written report on the matter with ASIC. In relation to a responsible entity, any breach relating to a scheme that has had, or is likely to have a material adverse effect on the interests of scheme members must also be reported to ASIC under section 601FC(1)(l) of the Act.

2.1. WHAT DOES “LIKELY TO BREACH” MEAN?

A licensee is likely to breach an obligation if, and only if, it is no longer able to comply with the obligation (s912D(1A)).

3. RESPONSIBILITIES IN RELATION TO BREACHES

All employees have a responsibility to comply with applicable financial services laws and internal policies. In the event that any of them becomes aware of a breach or a likely breach of any of these requirements, they must follow company procedures in relation to the reporting and management of the breach.

Managers have a responsibility to:

- (a) Identify and assess the severity of the breach or likely breach;
- (b) Report all breaches or likely breaches to the Compliance Officer;
- (c) Develop a proposed course of action to rectify the breach or prevent the likely breach occurring in consultation with the Compliance Officer, and after obtaining legal or other advice if appropriate;
- (d) Ensure that the appropriate corrective action has been taken to rectify the breach or likely breach and to prevent it from recurring; and
- (e) Co-operate with and assist in the reporting of breaches and likely breaches to the Board and, where necessary, ASIC, ASX, investors in the relevant fund and other stakeholders.

The Compliance Officer is responsible for recording and reporting breaches and likely breaches as follows:

- (a) Recording all breaches and likely breaches of which they are aware in the Breach register;
- (b) Investigating the circumstances of all reported breaches and likely breaches;
- (c) Reporting to the board:
 - All potentially significant breaches or likely breaches as soon as practicable, but no later than 4 business days after the licensee becomes aware of the breach or likely breach; and
 - All other breaches at least quarterly
- (d) Reporting all significant breaches or likely breaches to ASIC as soon as practicable but not later than 10 business days after the licensee becomes aware of the breach or likely breach.

The Compliance Officer will determine whether any breach or likely breach is potentially significant having regard to the factors contained in sections 912D(1)(b) and 601FC(1)(l) of the Corporations Act and after consultation with the General Counsel, the Audit and Risk Management Committee and/or the Board. If appropriate, the matter will be referred to an external party to obtain any necessary legal or other advice.

The Compliance Officer must report to the Board details of all breaches and likely breaches that are considered by the Compliance Officer to be potentially “significant” (as defined in the Corporations Act).

This report must be given to the Board as soon as possible, but in any event not later than 4 business days after becoming aware of the breach or likely breach, in order to allow time for the report to be made to ASIC within the 10 business day timeframe if necessary.

The Board, in consultation with the Compliance Officer and the General Counsel, and having regard to all the circumstances and any legal or other advice received, will determine whether a breach or likely breach that has been identified is required to be reported to ASIC.

3.1. WHEN IS A BREACH REQUIRED TO BE REPORTED TO ASIC?

A written report must be given to ASIC as soon as practicable, but within 10 business days of the licensee becoming aware of a breach or likely breach. This means that if, as an employee or representative of an AFS Licensee, you:

- breach any of the specified obligations under 912A and 912B of the Corporations Act; or
- are likely to breach any of the specified obligations under 912A and 912B of the Corporations Act; and
- the breach or likely breach is significant having regard to a number of prescribed factors,

you must immediately advise the Compliance Officer who will implement the process described above.

3.2. WHAT IS A SIGNIFICANT BREACH?

While the term “significant” is not defined in the Corporations Act, a number of factors can be used to determine whether a breach or likely breach is significant and therefore reportable to ASIC. A breach may be significant where only one of the factors applies to the circumstances surrounding the breach, or where there is a combination of factors.

The factors to be considered include:

1. The number or frequency of similar previous breaches.

The greater the number or frequency of similar breaches, the more likely the new breach will be significant. Repeated occurrences of a minor breach may amount to a significant breach and the repeat of a breach may also indicate a continuing underlying systemic problem.

2. The impact of the breach or likely breach on the ability of the licensee to provide the financial services covered by the license.

If a breach or likely breach reduces the licensee’s ability or capacity to provide the financial services covered by its AFS Licence, it may be significant. If the breach or likely breach does not affect the ability or capacity to provide the financial services covered by its AFS Licence, it may still be considered significant having regard to one or more of the other factors.

3. The extent to which the breach or likely breach indicates that the licensee's arrangements to ensure compliance with obligations is inadequate.

If the breach or likely breach indicates that the arrangements to ensure compliance are inadequate only in an isolated instance, it may not be considered significant. However, if it indicates broader inadequacies, it is more likely to be significant and should be reported. Questions should be asked about how long it took to discover the breach and to what extent the compliance arrangements helped in identifying the breach.

4. The actual or potential financial loss to the licensee or its clients arising from the breach or likely breach.

Any breach or likely breach that causes actual or potential financial loss to clients is likely to be significant. Where the breach is an isolated or occasional breach, the amount of the loss involved is minimal and immaterial, and the breach affects a very small number of clients, the breach is less likely to be significant.

If it is unclear as to whether the breach or likely breach is significant, in the first instance full details should always be reported to the Board to determine the appropriate course of action. It should be noted that failure to report a significant breach or likely breach is likely, in itself, to be a significant breach.

4. ACTION TO BE TAKEN FOLLOWING THE IDENTIFICATION OF A BREACH

Once a breach or likely breach has been identified, and irrespective of whether it is required to be reported to ASIC, the relevant manager, in consultation with the Compliance Officer, General Counsel and when appropriate with legal and other advisors, must:

- (a) Review the breach or likely breach to determine how and why it occurred;
- (b) Consider the consequences of the breach and, particularly, any effects for unitholders of the licensee;
- (c) Recommend corrective action to be taken, and implement the corrective actions decided upon;
- (d) Consider, make recommendations on, and implement as necessary, changes to practices or procedures intended to prevent similar breaches recurring; and
- (e) Assist in ensuring that all relevant parties are advised of the corrective action and any procedural changes undertaken, including, as necessary, the Board, ASIC and the Auditors.

4.1. HOW ARE RECORDS OF BREACHES MAINTAINED?

All breaches and likely breaches are reported to the Compliance Officer as soon as they are identified. The Compliance Officer logs all breaches into GRC Manager (an internet based program used to record and manage breaches and complaints) including the following information:

- (i) Date the breach or likely breach was identified;
- (ii) Name of licensee;
- (iii) Fund;
- (iv) Details of the breach;
- (v) Any actions taken to date;
- (vi) Root cause
- (vii) Any long term actions required to prevent similar types of breaches recurring
- (viii) Date breach was reported to the Board and, if applicable, ASIC

The Compliance Officer will ensure the effective management and rectification of the breach. Any documentation supporting the breach will be maintained by the Compliance Officer.

5. TRAINING

The Compliance Officer will ensure that all employees receive appropriate training on this policy at the commencement of their employment and on an ongoing basis.