ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM POLICY

1. Introduction

Coronation Fund Managers Ltd ("CFM") and its subsidiaries (collectively referred to as "the CFM Group") are committed to acting with integrity and in the best interests of stakeholders wherever we operate. We are committed to conducting our activities in accordance with all applicable laws and regulations relating to, inter alia, the combating of Money Laundering ("ML"), Terrorist Financing ("TF"), Proliferation Financing and Sanctions (collectively referred to as Anti-Money Laundering and Countering Financing of Terrorism ("AML/CFT")).

ML/TF are serious threats to the reputation, regulatory compliance and ultimately profitability of the CFM Group. Accordingly, we are committed to ensuring that the processes and controls which we have implemented are robust and effective enough to mitigate the risk of the CFM Group being abused for purposes of promoting ML/TF in South-Africa or elsewhere. These processes and controls should, at a minimum, include the following:

- Identification, assessment, monitoring, management and mitigation of ML/TF Risks by following a Risk-Based Approach ("RBA") in relation to compliance elements such as Client Due Diligence ("CDD");
- Identification of large, complex or unusual transactions by implementing risk-based transaction monitoring controls;
- Risk-appropriate internal controls, including to identify and report suspicious or unusual activities and transactions, as well as property linked to terrorism or to a sanctioned person;
- Effective recordkeeping measures;
- Ongoing training of relevant employees; and
- Developing, documenting, maintaining and implementing a Risk Management and Compliance Programme ("RMCP"), which includes elements of the above, as well as this Policy.

The CFM Board and senior management are responsible for ensuring that the CFM Group and its employees comply with the provisions of the Financial Intelligence Centre Act, 38 of 2001 ("FICA"). Section 42A of FICA requires the CFM Board and senior management to ensure that the risk-based processes and controls adopted by the CFM Group are appropriate and to appoint a person with sufficient competence and seniority to take responsibility for oversight of compliance with the processes and controls to identify and deter ML/TF Risks.

This Policy is a key component of CFM Group's RMCP and sets out the legislative and regulatory requirements with which the Accountable Institutions ("AIs") in the CFM Group must comply in order to manage and mitigate the ML/TF Risks it is exposed to through the offering of products and services. The AIs are collectively referred to as "Coronation" and currently consist of:

- Coronation Asset Management (Pty) Ltd;
- Coronation Investment Management International (Pty) Ltd;
- Coronation Alternative Investment Managers (Pty) Ltd;
- Coronation Management Company (RF) (Pty) Ltd; and
- Coronation Life Assurance Company Ltd.

This Policy must be read with:

- AML & CFT Business Risk Assessment (includes AML & CFT Risk Register, Client Risk Rating Methodology and AML & CFT Risk Factor Assessments)
- Apex Risk Management and Compliance Programme;
- Client Due Diligence & Ongoing Due Diligence Standard (includes PEP & client termination processes);
- Client Screening Standard;
- Transaction Monitoring & Reporting Standard;
- AML & CFT Recordkeeping Standard;
- AML & CFT Training Standard; and

- Client Due Diligence & Risk Rating Standard with respect to Beneficiaries of Insurance Policies

2. Applicable Legislation

This Policy takes account of the following legislation:

- FICA;
- Prevention of Organised Crime Act, 121 of 1998 ("POCA"); and
- Protection of Constitutional Democracy against Terrorist and Related Activities Act, 33 of 2004 ("POCDATARA").

3. Important Definitions

- **Money Laundering:** The FIC's Guidance Note 7 ("GN 7") states that ML is the manipulation of money or property in order to disguise its true source. In order to benefit from the proceeds of unlawful activity, criminals must conceal the origins of these funds. This is the process of ML. The result of a successful ML scheme is that proceeds of unlawful activity are no longer associated with the activity and appear to be legitimate income. There are three recognised stages in the ML process:

  a) "Placement" involves placing the proceeds of criminal conduct into the financial system.
  b) "Layering" involves converting the proceeds of criminal conduct into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds. This stage may involve transactions such as the subscription and redemption of units in collective investment schemes, and the buying and selling of stocks, commodities, or property.
  c) "Integration" involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

- **Terrorist Financing:** GN 7 states that the financing of terrorism involves the solicitation, collection and providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations or individual terrorists. The funds and assets may stem from both legal and illicit sources. The primary goal of persons involved in the financing of terrorism is to conceal both the financing and the nature of the activity being financed.

- **"Proliferation financing" or "proliferation financing activity":** FICA defines this as an activity which has or is likely to have the effect of providing property, a financial or other service or economic support to a non-State actor, that may be used to finance the manufacture, acquisition, possessing, development, transport, transfer or use of nuclear, chemical or biological weapons and their means of delivery, and includes any activity which constitutes an offence in terms of section 49A.

4. Requirements

4.1. Client Due Diligence

CDD refers to the information gathering process that Coronation conducts to gain knowledge about its clients and the nature of the business relationship. Section 21 of FICA requires Coronation to follow these steps:

- Identifying the client, any person on whose behalf the client is acting and any person who is acting on behalf of the client and verifying their identities by using reliable, independent source documents, data or information.
- Where relevant, identifying the Beneficial Owner of the client and taking reasonable measures to verify the identity of the Beneficial Owner, including taking reasonable measures to understand the ownership and control structure of the client.
- Obtaining information on the purpose and intended nature of the business relationship.
- In addition to CDD, after a client has been onboarded and funds invested, conducting Ongoing Due Diligence ("ODD"). This includes the monitoring of transactions undertaken throughout the course of the business relationship to ensure that the transactions being conducted are consistent with our

knowledge of the client, their business and risk profile and, where relevant, the Source of Funds ("SOF") and Source of Wealth ("SOW").

Coronation adheres to, and has implemented, the required CDD processes, which is described in more detail in the Client Due Diligence and Ongoing Due Diligence Standard.

4.2. Reporting Duties

Sections 28, 28A and 29 of FICA requires Coronation to report:

- cash transactions above a prescribed threshold;
- if Coronation finds itself in possession of terrorist property; and
- suspicious or unusual activities and transactions.

In order to achieve compliance with the FICA reporting obligations, Coronation has implemented appropriate ongoing screening and risk-based transaction monitoring controls. Transactions that are identified as not fitting the behaviour expected from a client risk profile, exhibiting red flags or deviating from the usual pattern of transactions, may be suspicious or unusual, must be reviewed and where required, reported to the FIC.

Please refer to the Transaction Monitoring and Reporting Standard for more details on Coronation's approach to transaction monitoring and reporting.

4.3. Recordkeeping

GN 7 states that recordkeeping is an essential component of a successful system to combat ML & TF and that meeting recordkeeping requirements will ensure that an AI captures adequate information to enable the reconstruction of a trail of transactions to assist investigators in determining flows of funds when performing their investigative functions. Accordingly, Section 22 of FICA requires Coronation to keep records of CDD information and transaction records respectively.

Please refer to the AML & CFT Recordkeeping Standard for more details on Coronation's approach to recordkeeping.

4.4. Training

Section 43 of FICA requires Coronation to provide training to employees to enable them to comply with the provisions of FICA and our RMCP. The effective application of Coronation's RMCP depends on the understanding by employees of the relevant requirements and accompanying processes they are required to follow and the ML/TF Risks these processes are designed to mitigate. The training of employees on FICA requirements and our AML/CFT processes are thus a key component of Coronation's RMCP.

Please refer to the AML & CFT Training Standard for more details on Coronation's approach to AML & CFT training.

4.5. RMCP

Coronation is required to develop, document, maintain and implement a RMCP to enable us to identify, assess, monitor, mitigate and manage our ML/TF Risks. Coronation has developed a RMCP which consists of this Policy and various Standards, Methodologies and operating procedures. All relevant employees must familiarise themselves and follow the RMCP.