

AML Policy (Anti-money Laundering, Counter Terrorist Financing and Counter Proliferation Financing Policy)



Table of Contents

1	DEFINITIONS AND ABBREVIATIONS	3
2	INTRODUCTION.....	4
3	POLICY SCOPE	4
4	POLICY DEFINITIONS AND REQUIREMENTS.....	5
	4.1 General definitions and requirements	5
	4.1.1 Money Laundering.....	5
	4.1.2 International Obligations and Responsibilities.....	6
	4.2 South African Board and AI responsibilities	6
	4.2.1 <i>Board responsibilities</i>	6
	4.2.2 <i>Management responsibilities</i>	7
	4.2.3 <i>Responsibility of Group Forensic Services (GFS) and Anti Money Laundering (AML) Operations</i>	7
	4.2.4 <i>Responsibility of Reporting Officer(s)</i>	7
	4.2.5 <i>Responsibility of Money Laundering Compliance Officer (MLCO)</i>	8
	4.2.6 <i>Responsibility of Compliance Function</i>	8
5	TRAINING	8
6	GOVERNANCE	8
7	NON-COMPLIANCE.....	8
8	ACCESS TO THE POLICY	9
9	POLICY REVIEW	9

1 DEFINITIONS AND ABBREVIATIONS

Accountable Institution/AI	A person referred to in Schedule 1 of the Financial Intelligence Centre Act No. 38 of 2001.
AML	Encompasses all operational processes in respect of managing the risk of money laundering (AML) and combating of financing of terrorist activities (CFT) and combating proliferation financing (CPF). Where the abbreviation AML is used it is inclusive of CFT and CPF.
Board	The Momentum Metropolitan Holdings Ltd Board of directors and/or Board of directors of an Accountable Institution.
Customer Due Diligence/CDD	The process through which the identity of prospective customers, including beneficial ownership is determined and verified as well as establishing and identifying various other details of clients and persons acting on behalf of clients on an ongoing basis taking in account the requirements of FICA.
DPEP	Refers to Domestic Politically Exposed Person.
Enhanced Customer Due Diligence/ECDD	Additional procedures performed over and above the Customer Due Diligence process when a client's or client's transactions are identified as carrying a "Higher Risk" for the potential of ML in terms of various personal, product and origin of business details.
FATF	Is a global inter-governmental body, that sets international standards for Combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.
FIC	Financial Intelligence Centre- The South African regulator appointed in terms of FICA.
FICA(A)	Financial Intelligence Centre Act No. 38 of 2001 and the FIC Amendment Act, No. 1 of 2017.
FPEP	Refers to Foreign Politically Exposed Person.
KYC	Know Your Client processes that includes the identification and verification of various client details and ongoing actions by clients. (Rules Based Approach)
ML	Money laundering can be described as the activity of concealing or disguising the nature, source, location, disposition or movement of the proceeds of crime.
MLCO	Money Laundering Compliance Officer.

MLRO	Money Laundering Reporting Officer.
MMH	Momentum Metropolitan Holdings Ltd, including its individual subsidiaries, operating divisions, business units, segments/channels, centres of excellence, product houses, licensed entities, management-controlled entities and activities.
PF	Refers to Proliferation Financing.
RMCP	Risk Management Compliance Program- An end-to-end program for managing the risk of money laundering and terrorist financing that includes a compliance programme as defined in terms of Section 42 of the FIC Amendment Act for a specific AI.
TF	Terrorist Financing is the financing of terrorism that involves the solicitation, collection and providing of funds and other assets with the intention that it may be used to support terrorist activities, terrorist organisation or individual terrorists. The funds and assets may stem both from legal and illicit sources.
WMD	Refers to Weapons of Mass Destruction.

2 INTRODUCTION

MMH is committed to the highest standards of compliance with anti-money laundering (AML) legislation and requires the Board, management and employees to adhere to high standards of preventing the use of MMH products and services for ML purposes or TF. The commitment is owned by the MMH Board of directors.

MMH will examine its AML strategies, goals and objectives on an ongoing basis and will always maintain an effective AML program that reflects the best practices for a diversified, global financial services provider.

Adherence to the MMH AML program is the responsibility of all employees. The MMH AML program consists of this MMH AML, Counter Terrorist Financing (CTF) and Counter Proliferation Financing Policy (CPF), and the AML Risk Management and Compliance Programme of each specific MMH Accountable Institution.

3 POLICY SCOPE

This policy applies to MMH Holdings Limited Accountable Institutions and subsidiaries and aims to establish and maintain high standards of responsible and ethical conduct within MMH related to the prevention of criminal activity, ML, TF and PF, by real or potential perpetrators by utilising products and services of MMH. This policy sets out the principles which must be adhered to by MMH employees, agents and contractors in order to comply with the applicable legislative obligations.

As a further MMH standard, all applicable laws need to be complied with in full.

4 POLICY DEFINITIONS AND REQUIREMENTS

4.1 *General definitions and requirements*

4.1.1 *Money Laundering*

Money laundering can be described as the activity of concealing or disguising the nature, source, location, disposition or movement of the proceeds of crime. It is the process of obscuring the illicit nature of criminal proceeds so that it can afterwards be spent without creating suspicion. Such criminal proceeds can be introduced by way of an investment into any of our products that is placed with product providers, and it ostensibly becomes "legal" when the investment is redeemed. The proceeds of crime include any asset (whether in cash or otherwise) which is obtained by virtue of criminal activities. This includes theft, robbery, fraud, abduction, extortion, dealing in drugs, evasion of tax, etc. Figuratively speaking, money laundering is the process of laundering "dirty" money, which can be used without creating any suspicion.

4.1.2 *Terrorist Financing*

Terrorist financing is the financial and logistical support, in any form, of terrorism or of individuals, entities or groups that encourage, plan or engage in acts of terrorism and includes plans or intended plans to support or commit an act of terrorism. It generally falls into two broad categories:

- Funding the direct costs associated with undertaking a terrorism act, for example expenses for recruitment, travel, explosive materials, weapons, vehicles and training, etc.
- Funding required to sustain a terrorist, a terrorist group, network or cell, either inside the country, transiting the country, or emanating from abroad.

The funds and assets may stem both from legal and/or illicit sources. The primary goal of persons involved in the financing of terrorism is to conceal the source of funds and assets, as with money laundering, but concealing both the financing and nature of the activity being financed.

4.1.3 *Proliferation Financing*

Proliferation financing (PF), refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

PF is confined to instances where funding is made available to or for the benefit of a person or entity whose name appears on a TFS list, due to the proliferation of WMD.

Proliferators use several evasive techniques and tactics to circumvent the financial sanctions Restrictions applied against them, providing them access to the financial system. Some key methods are:

- To avoid detection or distance themselves from certain transactions.

- Attempt to hide behind legal persons, trusts and partnerships.
- Utilise shell or front companies to obscure either the identity of the beneficial owner, the goods or activity being provided or the geographic area to the goods are destined.
- Hides the nature of the industry and the associated nature of goods he operates in.
- This risk could be further heightened, given the nature of the accountable institution's product offered to the client.

The primary goal is to make transactions look like normal commercial activity, structured to hide connections to proliferators or proliferation activities.

4.1.2 International Obligations and Responsibilities

South Africa is a member of the international Financial Action Task Force (FATF), focussing on combatting money laundering and terrorist financing. As such it is expected of the South African government and its citizens to provide visible and concrete commitment in managing the threats of money laundering, TF and PF.

Various MMH entities have the status of Accountable Institutions in terms of the Financial Intelligence Centre Act (FICA) and are required to adhere to the legislative obligations relating to AML, TF and PF.

4.2 South African Board and AI responsibilities

4.2.1 Board responsibilities

In terms of FIC Guidance Note 7 issued 2 October 2017 the following is imperative to note: -

“The board of directors, senior management or the person with the highest level of authority is ultimately responsible for ensuring that the institution maintains an effective internal AML/CFT/CPF control structure through a RMCP.

The board of directors or senior management must create a culture of compliance within the AI ensuring that the institution's policies, procedures and processes are designed to limit and control risks of money laundering and terrorist financing and are fully consistent with the law and that staff adhere to them.

The board of directors or senior management should be fully engaged in decision making processes and take ownership of the risk-based measures adopted since they will be held accountable if the content of the RMCP (or its application in the accountable institution) is found to be inadequate.”

In general, a financial services business or AI must ensure that there are appropriate and effective policies, procedures and controls in place which provide for the Board to meet its obligations relating to compliance review, in particular the Board must: -

- Ensure that the compliance review policy takes into account the size, nature and complexity of the business and includes a requirement for sample testing of the effectiveness and adequacy of the policies, procedures and controls including where aspects of the due diligence process are undertaken via electronic methods and systems;
- Consider whether it would be appropriate to maintain a separate audit function to assess the adequacy and effectiveness of the area of compliance;

- Ensure that when a review of compliance is discussed by the Board at appropriate intervals the necessary action is taken to remedy any identified deficiencies;
- Ensure that the financial services business is meeting its obligation, that its branches and subsidiaries operating outside South Africa comply with the Regulations and applicable local law which is consistent with the FATF recommendations;
- Provide adequate resources either from within the financial services business, within the group, or externally to ensure that the AML/CTF/CPF policies are adhered to.

4.2.2 Management responsibilities

Management must assist the MMH Board and boards of Accountable Institutions to ensure that an AML/TF Risk Management Compliance Program (RMCP) is embedded. A RMCP is a defined record of an AI's control measures and efforts to comply with its obligations under the FICA Act on a "risk based" basis.

Below follows the minimum requirements of a RMCP: -

- A documented, maintained and implemented program to manage the risk and the compliance obligations of an AI that incorporate all the elements of a comprehensive and effective AML Risk Based Client Due Diligent process (CDD).

The program will incorporate the application and implementation of measures of that will as a minimum include: -

- The end-to-end CDD process, i. e. from establishing a business relationship, on-boarding a client, engaging in transactions, ongoing monitoring of client behaviour, to termination of the relationship with recordkeeping of all relevant client detail and transaction information.
- Measure to deal with a client identified as a DPEP/PIP/FPEP.
- Ongoing CDD processes in dealing with High-Risk clients or status changes in a client's risk profile from Low to High Risk.
- Measures to deal with doubt about the veracity of previously obtained CDD information.
- Measure to deal with suspicion formed of ML or TF activities formed post client on boarding.
- Measures to prevent or entering into or maintaining business relationships or concluding transactions if an AI cannot perform CDD and the manner in which an AI will terminate an existing business relationship when unable to complete CDD requirements, etc.
- Describe in detail all implanted governance processes, for example processes related to executing reporting obligations, training programs, compliance monitoring programs etc.

4.2.3 Responsibility of Group Forensic Services (GFS) and Anti Money Laundering (AML) Operations

GFS and AML Operations will assist business in implementing standardised MMH and individual business processes and controls in order to mitigate ML/TF/PF risk across MMH.

4.2.4 Responsibility of Reporting Officer(s)

The Money Laundering Reporting Officer (MLRO) has a responsibility and authority to monitor and maintain all the AI information on the go-AML messages board and to *inter alia* complete and submit intelligence reports to the FIC via go-AML web reporting tools that includes reports relating to cash receipts (above the regulated

amount), suspicious and unusual transactions activities, transactions or activities relating to financing of activities linked to terrorism as well as responding to specific requests from the FIC.

4.2.5 Responsibility of Money Laundering Compliance Officer (MLCO)

The MLCO should be sufficiently competent and have seniority to assist the Board(s) and senior management in discharging their obligations under FICA.

The MLCO will be responsible for:

- Ensuring that an appropriate AI specific AML Risk Management and Compliance Program is in place and adhered to by business;
- Ensuring that ongoing monitoring and reporting transpires within each business area to establish the effectiveness and efficiencies of the RMCP
- Ensuring corrective action is enforced where weak and unsteady processes were identified
- Providing independent oversight and guidance to business in respect of the AML Risk Management Compliance Program
- Providing independent assurance to the board and other stakeholders on the effectiveness of the management of AML compliance risk

4.2.6 Responsibility of Compliance Function

Compliance with this Policy and the AML Risk Management and Compliance Programme will be monitored by Group and business Compliance. Compliance will report to the relevant boards on and recommend, where applicable, on improvements required based on the monitoring results. It remains the responsibility of AI management to take appropriate action based on these recommendations and findings. The Compliance function will assist business in interacting with Regulators in respect of AML compliance matters.

5 TRAINING

General awareness training on anti-money laundering will be provided to all employees of MMH. Employees who work directly with customers and those employees in essential auxiliary functions that may be exposed to money laundering and terrorist financing threats will receive detailed process and product specific training to enable them to assist MMH in managing money laundering risk.

6 GOVERNANCE

The MMH Board of Directors assumes overall responsibility for the total processes of the AML Policy and individual AI Risk Management Compliance Programs as to ensure that AML risk management and compliance is embedded in the organisation's culture.

This policy derives its authority from the MMH Board of Directors under the oversight and approval of the MMH Board Risk, Capital and Compliance Committee and the MMH Group Executive Committee.

7 NON-COMPLIANCE

Non-compliance with this Policy or any AML Risk Management and Compliance Program will result in disciplinary action and possible dismissal.

8 ACCESS TO THE POLICY

Access to this policy is to be provided to all MMH employees, agents and contracted individuals who engage on behalf of MMH with clients or potential clients or deal with client transactions and/or business relationships of clients with MMH.

9 POLICY REVIEW

This policy is to be reviewed annually by MMH Group Compliance and MMH AML Operations and input must be provided by AI's. The policy must be ratified by the MMH Board.