MountHurst™ Wealth

Compliance – AML, CTF Policy

Anti-Money Laundering & Counter-Terrorist Financing Policy

Policy on Prevention of Money Laundering and Terrorist Financing

Policy on Prevention of Money Laundering and Terrorist Financing

MOUNTHURST™ Group

Version 1
2017

Table of Content **Pages**

DEFINITIONS

The **MountHurst™** Group's Anti-Money Laundering Policy covers all activities designed to protect the Group from being used as a medium for facilitating illegally obtained money from sources including illicit trafficking in narcotic drugs and psychotropic substances, participation in an organized criminal group, illicit arms trafficking, corruption, smuggling, fraud and robbery or theft, embezzlement or any other criminal activities.

The Policy also covers Terrorism and Terrorist act and defines them as any act that is "aimed at killing or severely injuring a civilian or any other individual who does not participate directly in an armed conflict; if by nature or due to the circumstances, such an action aims at intimidating a population or forcing a government or an international organisation to take or refrain from taking a given action."

WHY A POLICY?

Money laundering has become a major international problem. In cash intensive economies such as obtains in our region, illegal money can easily be integrated into the financial system. Our countries also are exposed to drug trafficking, embezzlement and racketeering.

As far as terrorism is concerned, the increased incidence of terrorist acts at the international level has necessitated appropriate preventive and repressive measures to stop their financing. Therefore, financial institutions are expected to participate actively and strongly in the implementation of measures aimed at, among others, freezing of funds and other financial assets owned by individuals or organisations that commit or participate in terrorist acts. **MountHurst™** Group addressed very early the need to protect itself and its staff against Money Laundering and Terrorism Financing activities and their consequences.

MountHurst™ Group has approved an "Anti-Money Laundering Policy" for implementation in all the operating units of the Group. This policy was adopted in line with "Rules of Business Ethics" for Directors and Staff, setting the pace for true ethical practices in the Group.

RECENT DEVELOPMENTS

Money laundering methods and techniques are constantly changing. The "Anti-Money Laundering Policy," of the Group accordingly deals particularly with diligences relative to the identification of the client or the ultimate beneficiary of any operation, as well as the reporting of all individuals and institutions officially listed by the international community as suspected sponsors of terrorism.

Where the requirements of the Anti-money Laundering and Anti-Terrorism Financing Policy are not met subsidiaries will not commence business relations or perform any transaction. In the event that there is an existing business relationship, such relationship would be terminated and a report made to the relevant authorities

1. INTRODUCTION

'This policy document has been prepared by **MountHurst™** Group to outline practice policy for the implementation of the risk based approach for Anti-Money Laundering/Counter-terrorist financing (AML/CTF) and controls for AML/CTF. The practice is committed to upholding its AML/CTF obligations under the Proceeds of Crime Act 2002 (as amended), the UK Money Laundering Regulations 2007 as amended and the Terrorism Act 2000 (as amended)

MountHurst™ Group is committed to the highest standards of anti-money laundering (AML) & counter-terrorist financing (CTF) compliance and requires management and employees to adhere to these standards to prevent use of our recommended products and services for such purposes.

MountHurst™ Group will examine its Anti Money Laundering strategies, goals and objectives on an ongoing basis and maintains an effective Anti-Money Laundering program for the group's business that reflects the best practices for a diversified, global financial services provider.

Adherence to the **MountHurst™** Group Anti-Money Laundering & Counter-Terrorist Financing Policy is the responsibility of all employees. The policy is formulated and directed by the Group Head of Anti Money Laundering. The policy includes client screening and monitoring requirements, "know your customer" policies (including the requirement to establish the identity of beneficial owners), record keeping requirements, the reporting of suspicious circumstances in accordance with relevant laws, and AML training.

The Policy also covers Terrorism and Terrorist act and defines them as any act that is "aimed at killing or severely injuring a civilian or any other individual who does not participate directly in an armed conflict; if by nature or due to the circumstances, such an action aims at intimidating a population or forcing a government or an international organisation to take or refrain from taking a given action."

All staff must read and become familiar with this policy document and the guidelines upon joining the practice and be aware of their own personal legal obligations'

2. SCOPE

2.1 Objectives

The standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements and apply for the entire **MountHurst™** Group. These requirements are intended to prevent **MountHurst™** Group members, employees and clients from being misused for money laundering, terrorist financing or other financial crime. This Policy establishes the general framework for the fight against money laundering and financing of terrorism.

2.2 Applicability

Wherever local regulations are stricter than the requirements set out in this Policy, the stricter standard has to be applied. If any applicable laws are in conflict with this Policy, the relevant **MountHurst™** Group entity must consult with the local legal department and the Group Head of Anti Money Laundering to resolve the conflict.

If the minimum requirements set out in this Policy cannot be applied in a certain country because application would be against local law or cannot be enforced due to other than legal reasons, **MountHurst™** Group has to assure that it will not

- ***enter into a business relationship,***
- ***continue a business relationship or***
- ***carry out any transactions.***

If business relations already exist in that country, **MountHurst™** Group has to assure that the business relationship is terminated regardless of other contractual or legal obligations.

2.3 Definition of the term Money Laundering

Money Laundering is the introduction of assets derived from illegal and criminal activities (Predicate offences) into the legal financial and business cycle. Offences are for example forgery of money, extortionate robbery, drug crime as well as fraud, corruption, organised crime, or terrorism etc. Predicate offences for money laundering are defined by local law. Generally speaking, the money laundering process consists of three "stages":

- **Placement:** The introduction of illegally obtained monies or other valuables into financial or non- financial institutions.

- **Layering:** Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

- **Integration:** Placing the laundered proceeds back into the economy in such a way that they re- enter the financial system as apparently legitimate funds.

These "stages" are not static and overlap broadly. Financial institutions may be misused at any point in the money laundering process

3. MINIMUM REQUIREMENTS

All **MountHurst™** Group branches and subsidiaries have to comply with the following basic principles:

3.1 Client Due Diligence (CDD)

I. **CDD** must be carried out on new clients before starting to provide services or otherwise in accordance with the provisions of regulation 9 of the Money Laundering regulations 2007.

II. Client acceptance checklists will be prepared for all clients to provide all the relevant information which must include original documentary evidence of identity and proof of address which must be verified independently. Refer to **Annex 1** for types of identification documents required for all client types.

III. Where clients or client representatives are not met face-to-face, ***ENHANCED DUE DILIGENCE*** processes must be followed as outlined below

IV. Clients must be checked for **POLITICALLY EXPOSED PERSON** status (PEP). Checks may include:

- a written declaration from the client that they are or are not a Politically Exposed Person once they have read the definition, and/or;
- an online or database electronic verification check.

V. Services must be declined if it appears that the client is being deliberately difficult in providing information for **CDD**.

VI. Special attention must be paid to correspondent business and adequate security measures must be implemented.

VII. It is **MountHurst™** Group policy to update CDD information **annually** for standard/low risk clients, to ensure that information is up to date and in accordance with the requirements of regulation 7 of the ML regulations 2007.

3.2 Enhanced Due Diligence Measures (EDD)

I. **EDD** measures to be applied include ensuring that the customer's identity and source of funds/wealth is-verified by additional documents, data or information such as those outlined in Annex 1

II. Additional processes should include **at least** one additional document from Annex 1 or one or more of the following: **[*obtaining certified copies of identification / proof of address; an electronic database check; communicating***

***with the client in writing at their verified/confirmed residential address and requiring them to return a completed or signed/acknowledgement without alteration*].**

III. Higher risk clients must be subjected to more frequent and in-depth scrutiny of activity and source of funds/wealth/income.

4. BENEFICIAL OWNERSHIP

Identification of Ultimate Beneficial Owner: Whenever **MountHurst™** Group is required to identify a client; it must establish and verify the identity of the ultimate natural person,

- who owns or
- controls the client or its assets or
- on whose behalf the transaction is carried out or the business relationship is established

I. Clients must be checked for the existence of any beneficial owners

II. Where applicable, names, dates of birth and addresses of all beneficial owners must be received and recorded by the relevant staff member responsible for the client relationship acceptance or sign-off

III. In higher risk cases, staff must verify the identities of such beneficial owners, including refer to Companies House website (incl. Persons with Significant Control (PSC) register) to verify the ownership and control structure of entities and may also supplement this process with checks using additional face-to-face meetings to verify the identity of beneficial owners.

5. ONGOING MONITORING OF CLIENTS

A permanent monitoring of clients' accounts must be implemented to detect unusual/suspicious transactions. Monitoring must be effected for applicable business areas using adequate processes and systems.

I. We have an obligation to scrutinise transactions, services provided/requested, source of funds and other elements of knowledge collected in the customer due diligence process, to ensure the new information is consistent with other knowledge of the client. We also have a duty to keep the documentation concerning the client and the relationship update to date.

II. Should the client request additional or different services it may be necessary to carry out new or enhanced client due diligence checks to ensure that the practice has a good understanding of the source of wealth, the source of funds or the intended purpose of the new relationship

III. CDD checks including identification documents will be refreshed **every 5 years** to ensure that documents remain valid and up-to-date

6. SUSPICIOUS ACTIVITY REPORTING

Such circumstances/transactions must be reported to the competent authorities according to local law. Group Anti Money Laundering must be informed about all suspicious events, if not explicitly prohibited by local law

I. All staff must report knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or terrorist financing. This is a **personal obligation** for every member of staff and failure to do so is an offence punishable by **up to 5 years imprisonment.** Internal reports should be made in writing by email directly to the Group Head of Anti Money Laundering.

II. The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted will be recorded in a **confidential and separate place from the client file**, with sufficient details and reasons for the course taken, for a period of **5 years**.

III. All staff must be aware that it is an offence to disclose that a Suspicious Activity Report (SAR) to the NCA has been made about a client, punishable by **up to 5 years imprisonment.** (Tipping-off offence – Proceeds of Crime Act section 333A).

7. TRAINING

All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships must undergo anti money laundering training. **MountHurst™** Group has decided to extend the target audience for AML to cover all staff. Initial training must be attended within three months after an employee has joined **MountHurst™** Group and subsequently every two years. Minimum content training requirements

I. All staff must receive training/training manuals on their AML/CTF obligations and how it relates to their day-to-day duties. Training will be provided Group Head of Anti Money Laundering to all new staff. Refresher training will be provided **every two years** after an incident or breach, following regulatory changes or otherwise on a risk-sensitive basis to be determined by management and MLRO.

II. Records of attendance lists and dates of training must be kept and details of what was covered in the session included.

8. RECORD RETENTION

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to money laundering topics (e.g. files on suspicious activity reports, documentation of AML account monitoring, etc.). Those records must be kept for a minimum of **6 years**.

The following records must be kept **for 6 years** from date we stop providing services to the client (i.e. end of the business relationship);

I. **CDD/EDD** documentation and supporting information

II. Training records for all relevant staff

III. Records of internal suspicious transactions reports (if applicable)

IV. Records of any Suspicious Activity Reports (SAR) made to the NCA and reasons for the report are also to be kept for 6 years and should be recorded separately from the client file.