MAC & RO CAPITAL FZC

AML/CFT POLICIES & PROCEDURES

CONFIDENTIALITY STATEMENT

POLICY STATEMENT

Mac & Ro Capital FZC is a licensed entity and supervised by the Ministry of Economy as its reporting entity and is committed to prevent money laundering and countering the financing of terrorism.

MAC & RO CAPITAL FZC is engaged in the Non-Manufactured Precious Metal Trading, Precious stones, Pearls, & Precious Metal Trading.

The management understands the importance of application of the standards and guidelines issued by the Ministry of Economy and the supplementary guidance for industry best practices while doing the transactions and conducting businesses in the UAE.

The management of **MAC & RO CAPITAL FZC** believes that the best way to fulfil this commitment is to establish effective internal policies and procedures that are conducive to:

- Carrying out the activities and services provided in accordance with strict ethical standards and current laws and regulations.
- The implementation of codes of conduct and monitoring and reporting systems to prevent that, the company is used for money laundering and terrorism financing.
- Ensuring that all the employees of **MAC & RO CAPITAL FZC** observe this policy manual and perform action to the adherence of the process mentioned in it.

This Policy Manual is constituted by:

Please also refer to the following procedures manuals as part of the AML CFT Policy and

Procedures:

All Policies name

i. AML/CFT Governance Framework
ii. Suspicious Transactions Reporting (Procedures)
iii. Suspicious Transactions Reporting (Procedures)
iv. Risk Identification & Assessment
v. Red Flags Indicators

Reviewed and recommended by:	**Approved by:**
Compliance Officer/ MLRO	**Manager**
Date:	**Date:**

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

MAC & RO CAPITAL FZC (herein referred to as "the Company") is a legal entity that was established and registered in Sharjah, United Arab Emirates (UAE).The business activity of the company is to engage in Non-Manufactured Precious Metal Trading, Precious stones, & Precious Metal Trading.

The company operates within the UAE and may also engage in international trade.

As a legal entity, **MAC & RO CAPITAL FZC** must comply with local and international regulations concerning the conduct of its business. This includes adherence to relevant laws and regulations related to the purchase and sale of gold and other precious metals. The company must also maintain appropriate records of its transactions, customer information, and due diligence measures undertaken.

1.2 PURPOSE

This policy has been formed in the light of FIU Regulations, Circulars & Notifications on Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT).

In pursuance of the:

-Federal Decree-Law No. (20) of 2018,

-Cabinet Decision No. (10) of 2019,

-Cabinet Decision No. (58) of 2020, and related circulars & notifications by the Ministry of Economy (MOE);

The policy of the company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or terrorist financing. Money Laundering (ML) is generally understood as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds or assets so that they appear to have been derived from legitimate origins or constitute legitimate assets.

The purpose of this policy is to establish the general framework within **MAC & RO CAPITAL FZC** for the fight against money laundering (ML) and financing of terrorism (FT). This Policy sets out those provisions, procedures, and controls as enacted by **MAC & RO CAPITAL FZC** concerning Anti-Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT").
The rationale behind the Policy is crystal clear **MAC & RO CAPITAL FZC** will only accept those business associates/ clients/ customers; whose sources of precious metals or funds can be reasonably established as legitimate; and that do not pose any risk (actual or potential) to **MAC & RO CAPITAL' s** reputation.

Considering the foregoing, **MAC & RO CAPITAL FZC** will not tolerate any involvement in illegal activities or unauthorized activities by its staff, business associates/ clients/ customers.

Initiatives by MAC & RO CAPITAL FZC

a) Registered in the Financial Intelligence Unit (Go AML) portal.
b) Implemented a sanction screening system
c) Appointed a Compliance Officer
d) Conducts Due Diligence on clients by verifying the identity of customer and beneficial owner before establishing a business relationship or opening an account.
e) Ensures Compliance with sanctions screening and reports any suspicious activity.

MAC & RO CAPITAL FZC will be reporting through online Go-AML portal provided by the FIU.

All reporting to be done at the time of receiving the funds. Reporting to be done within 2 weeks of occurring the qualifying transactions.

The basic purpose of the AML Policy is to establish a system for **MAC & RO CAPITAL FZC** to participate in the international efforts against ML and to duly comply with the guidelines as detailed in the various circulars & notifications of FIU, and other legal provisions and to ensure that **MAC & RO CAPITAL FZC is** not used as a vehicle for ML. The AML framework of **MAC & RO CAPITAL FZC** would meet the extant regulatory requirements.

We confirm that we are observing and complying with domestic and international laws, rules and regulations, including those governing the illicit trade in precious metals and the United Nation Security Council (UNSC) sanctions.

1.3 SCOPE

This Policy is applicable to all employees of **MAC & RO CAPITAL FZC** suppliers, customers and third parties that we deal with. It applies to all the following dealings:

- Precious metals mean gold, silver, palladium, or platinum whether in coins, bars, ingots, granules or in any other similar form.
- Precious stones mean diamonds, sapphires, emeralds, tanzanite, rubies, or alexandrite.
- Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment, such as earrings, bracelets, rings, necklaces, brooches, watches, etc.
- Any object concerning which at least 50 percent of its monetary value is comprised of precious metals and stones (PMS)
- A variety of high-value industrial metals, including so-called conflict minerals (for example, wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g., rhodium, etc.);
- A variety of semi-precious gemstones (e.g., amethysts, opals, jade, and others);
- Synthetic, treated, or artificial gemstones (Diamonds, Emeralds, Rubies, Sapphires, Pearls).

This Policy is applicable to production and/or trade of precious metals or stones, whether in raw, cut, polished, or elaborated (mounted or fashioned) form. Production and/or trade in this context includes any of the following acts involving raw/rough or processed/finished PMS:

- Extraction (whether by mining or other method), refining, cutting, polishing or fabrication.
- Import or export.
- Purchase, sale, re-purchase, or re-sale (whether in primary, secondary, or scrap markets);
- Barter, exchange, or other form of transfer of ownership.
- Loan or lease arrangements (e.g., sale-leaseback, consignment, or memorandum sales);
- Possession (whether permanent or temporary, for example, as part of a fiduciary, warehousing, collateral, or other safekeeping arrangement; or under contract for a specific purpose such as cutting, polishing, refining, casting, or fabrication services).

This Policy is applicable to:

- Wholesale or Retail Trade
- Whether it is direct or indirect (such as through a broker or other intermediary)
- Whether it is between natural or legal persons or legal arrangements, including any other Dealer in precious metals and stones (DPMS)
- Whether the PMS are traded physically or virtually (for example, via certificates, on electronic exchanges, or via internet), irrespective of where or by whom the physical goods are warehoused, held in safekeeping, or delivered.

2. DEFINITION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

2.1 DEFINITION OF MONEY LAUNDERING

Money Laundering (ML) is the process of converting the illegal money or the proceed of crime (the Money acquired, whether directly or indirectly, in whole or in part, from any criminal activity) into clean money so as to conceal the source / origin of fund.

Money Laundering crimes are defined as under Article (2) of the Decree Law:

- Any person, having the knowledge that the funds are the proceeds of a felony or a misdemeanor, and who willfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:
    - *Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source.*
    - *Concealing or disguising the true nature, source, or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.*
    - *Acquiring, possessing, or using proceeds upon receipt.*
    - *Assisting the perpetrator of the predicate offense to escape punishment.*

The crimes of Money Laundering are considered to be an independent crime. The punishment of the perpetrator for the predicate offence shall not prevent his punishment for the crime of Money Laundering.

The process of laundering money typically involves three steps: ***placement, layering, and integration.***

- **Placement:** The physical disposal of cash or other assets derived from criminal activity.
- **Layering:** The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.
- **Integration:** Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

2.2 DEFINITION OF FINANCING OF TERRORISM

Terrorism is the act of seeking for political, religious, or ideological reasons to intimidate or compel others to act in a specified manner. The process of making finances or other assets accessible to support, even indirectly, terrorist actions is known as terrorism financing. These offenses include using or possessing money or other property for terrorist purposes, as well as participating in fundraising arrangements to support terrorist actions. The definition of financing of terrorism is as follows:

- any person who willingly collects or provides funds, directly or indirectly and by any means, with the knowledge that such funds will be used in full or in part, to carry out a terrorist act, or by a terrorist individual or a terrorist organization, shall be deemed to have committed the offense of terrorism financing.
- Such provisions include financing the travelling of individuals to a country other than their country of residence or nationality with the intent to perpetrate, plan, prepare for, participate to, or facilitate terrorist acts, or provide necessary funds for training on terrorist acts or receiving such training.

There are three stages to terrorism financing that are typically followed: -

(1) Raising funds through donations, self-funding, microloans, or criminal activity is one method of raising funds.
(2) Making a financial transfer to a terrorist, terrorist network, terrorist organization, or terrorist cell.
(3) The funds could be used for a variety of purposes, such as purchasing weapons or bombs, making payments to terrorists or insurgents, or funding the expenses of terrorist organizations.

3. AML/CFT COMPLIANCE PROGRAM

The Pillars of our AML/CFT and Sanctions Compliance include:

A. Adoption of Risk Based Approach
B. Assessment of Entity-Wide Risks and Client Risks
C. Implementation of Risk-based Procedures and Internal Control to prevent and deter ML/TF and Sanctions Avoidance
D. Undertaking Customer Due Diligence for all clients and Enhanced Due Diligence for High-Risk Clients and PEPs
E. Appointment of a Compliance Officer
F. Employee Screening and Staff Training
G. Dissemination of Suspicious Activity Indicators to employees
H. Identification of Suspicious Activity and reporting of Suspicious activity to the Financial Intelligence Department through GOAML Portal
I. Record-keeping
J. Adherence to Sanctions Compliance
K. Independent Review of AML/CFT/Sanctions Compliance program

4. STATUTORY PROHIBITIONS

MAC & RO CAPITAL FZC commits that it will not:

A. Establish or maintain any Customer or Business Relationship or conduct any financial or commercial transactions with any natural or legal person who is anonymous or known by fictitious name or by pseudonym or number.
B. Establish or maintain a Business Relationship or execute any transaction in the event we are unable to complete adequate risk based CDD measures in respect of the Customer for any reason.
C. Deal with Customers listed under any Sanction watchlist and/or United Nation's "Consolidated List" and UAE Local Terrorist list.
D. Invoke professional or contractual secrecy as a pretext for refusing to perform our statutory reporting obligation with respect to suspicious activity.

5. OBJECTIVES

a) To establish a framework for adopting appropriate AML Procedures and controls in the operations / Business processes of **MAC & RO CAPITAL FZC**
b) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
c) To comply with applicable laws and regulatory guidelines.
d) To take necessary steps to ensure that the concerned staff is adequately trained and KYC/AML procedures are implemented.
e) To assist law enforcement agencies in their effort to investigate and track money launderers.

6. COMPANY'S COMMITMENT

MAC & RO CAPITAL FZC is a company registered under **SAIF INDUSTRIAL ZONE OF SHARJAH, UAE.** The company deals in trading of Precious Metal Trading, Precious stones, and Non-Manufactured Precious Metal Trading, The Company is covered under the United Arab Emirates Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML/CFT Law").

As per this law, the company is obligated to establish a set of policies and procedures to ensure that it does not participate or facilitate money laundering and/or the financing of terrorists or criminal activities.

MAC & RO CAPITAL FZC is strictly committed to adhere to the policies, rules, regulations and guidance provided by the Government of UAE.

MAC & RO CAPITAL FZC continue to train its staff on the vulnerability of the DPMS sector and based on the regulations on the anti-money laundering and combating financing of terrorism & criminal activities with a specific emphasis on the KYC (Know Your Customer) and Due Diligence Principle. Our staff are also encouraged to participate in the various seminars organized by the various authorities and local bodies such as SAIF ZONE' workshops in Sharjah.

We commit to rejecting or immediately suspending and discounting engagement with suppliers or customers where we identify a reasonable risk that they are sourcing (or are linked) to parties committing any of the crimes described above.

We will not tolerate any direct or indirect support to non-state armed groups or their affiliated who:

- Illegally control mine sites, transportation routes or other points in the supply chains.
- Illegally tax or extort money or minerals at points in the supply chain, such as mining sites, or points where minerals are traded or exported.

The issuance of this Policy together with the implementation, operation, and enforcement of the procedures and controls therein, reflect **MAC & RO CAPITAL FZC's** commitment in this regard.

To combat money laundering and/or the financing of terrorism **MAC & RO CAPITAL FZC** shall co-operate with UAE and international government agencies, and recognized law enforcement agencies.

7. AML/CFT PERTAINING TO PRECIOUS METALS & STONES INDUSTRY

7.1 DEFINITION OF PRECIOUS METALS AND STONES (PMS)

Definitions of precious metals and precious stones may vary somewhat depending on region. Mostly accepted classifications internationally, based the quality, intrinsic value, and rarity, consider the precious metals to consist of gold, silver, and the so-called platinoid metals (principally platinum and palladium); and precious stones to consist of diamonds, emeralds, rubies, and sapphire. Pearls are often also included in the category of precious stones and are thus included in the supplemental guidance issued by the Regulator.

These generally accepted classifications are reflected in the federal legislation of the UAE, which governs the control, stamping and identification of PMS, as well as the import and export requirements concerning raw precious stones under the internationally accepted Kimberley Process Certification Scheme. The Broad definitions of precious metals and precious stones considered in the supplemental guidance include, but are not limited for Materials falling under the following categories:

I. PRECIOUS METALS

- Gold, with a minimum purity of 500 parts per 1,000;
- Silver, with a minimum purity of 800 parts per 1,000;
- Platinum, with a minimum purity of 850 parts per 1,000;
- Palladium, with a minimum purity of 500 parts per 1,000.

II. PRECIOUS STONES

- Precious stones (rough) of any weight in carats;
- Precious stones (polished), with a minimum weight of 0.3 carats per stone if loose, or a minimum weight of 0.5 carats per any single stone mounted in a setting (whether of one or more stones);
- Colored Gemstones (polished Emeralds, Rubies, Sapphires), with a minimum weight of 1 carat per stone if loose, or a minimum weight of 2 carats per any single stone mounted in a setting (whether of one or more stones).
- Pearls
- Loose, with a minimum diameter of 3 millimeters per bead;
- Strung or mounted in a setting (whether of one or more beads), with a minimum diameter of 10 millimeters per any single bead.

III. OTHERS

- The above definitions notwithstanding, for the purpose of applying AML/CFT measures in respect of covered transactions, PMS to include any object concerning which at least 50 percent of its monetary value is comprised of PMS.
- Furthermore, it should also be recognized that DPMS may engage in transactions involving other types of metals and gemstones (whether traded regularly or occasionally, and whether

physically or through electronic or virtual exchanges) which, while technically not considered to be PMS (although they may be of high value in some cases), may nevertheless be subject to risks of ML/FT or other predicate offences (e.g., fraud) similar to PMS. Such materials may include:

- A variety of high-value industrial metals, including so-called conflict minerals (for example, wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g., rhodium, etc.);
- A variety of semi-precious gemstones (e.g., amethysts, opals, jade, and others);
- Synthetic, treated, or artificial gemstones (diamonds, emeralds, rubies, sapphires, pearls).

7.2 OBLIGATIONS FOR DEALERS IN PRECIOUS METAL & STONES (DPMS)

Cabinet Decision no. (10) of 2019 concerning the implementing Regulation of Decree Law no. (20) of 2018 on Anti-money laundering and Combating the financing of terrorism and Illegal organizations (the AML/CFT decision), identifies the dealers in precious metals & stones (DPMS) as Designated Non-financial Business & Professions (DNFBPs), when they engage in carrying out any single monetary transaction, or several transactions which appear to be interrelated, whose value is equal to or greater than AED 55,000; and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates (UAE).

The principal obligations of **MAC & RO CAPITAL FZC** under the AML-CFT Law, AML-CFT Decision and Related Resolutions relate to the following categories of actions:

- Maintaining a continuously up-to-date awareness of the persons and organizations listed in the relevant Sanctions Committees lists and comparing these on an ongoing basis with their customer databases.
- Ensuring, prior to entering business relationships or conducting any transactions with natural or legal persons or legal arrangements, that such persons or organizations are not included in the relevant Sanctions List;
- Freezing (or unfreezing when so instructed by the Competent Authorities) the Funds of listed persons or organizations, which the supervised institutions hold, have access to, or otherwise control'
- Immediately reporting to the Supervisory Authorities when listed persons or organizations are identified and/or when the Funds of such persons or organizations are frozen, as well as in other specific situations stated in AML-CFT Law.

8. STAGES OF MONEY LAUNDERING

i. Placement

This is the first stage of money laundering is known as ‘placement’, whereby ‘dirty’ money is placed into the legal, financial systems. After getting hold of illegally acquired funds through theft, bribery and corruption, financial criminals move the cash from its source. This is where the criminal money is ‘washed’ and disguised by being placed into a legitimate financial system,

Examples of Placement

1. Blending of funds.
2. Invoice fraud.
3. Through 'smurfing'.
4. Offshore Accounts.
5. Carrying Small Sums of Cash Abroad.
6. Through Aborted Transactions.

ii. Layering

The second stage in the money laundering process is referred to as 'layering'. This is a complex web of transactions to move money into the financial system, usually via offshore techniques. Once the funds have been placed into the financial system, the criminals make it difficult for authorities to detect laundering activity. They do this by obscuring the audit trail through the strategic layering of financial transactions and fraudulent bookkeeping.

iii. Integration

The third of the stages of money laundering is 'integration'. The 'dirty' money is now absorbed into the economy, for instance via real estate. Once the 'dirty' money has been placed and layered, the funds will be integrated back into the legitimate financial system as 'legal' tender.

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

9. APPLICABLE LAWS AND REGULATION

9.1 OVERVIEW

The Company has developed and implemented this AML & CFT Policy, in line with the self-assessment of inherent ML/TF risk in nature of business activities, National Risk Assessment, National Legislative and Regulatory framework as the base in conjunction with the below listed legislations, resolutions, notices, and circulars.

9.2 LISTING OF APPLICABLE LAWS AND GUIDANCE

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML-CFT Law");
- Federal Decree No. (26) of 2021 amending certain provisions of Law No.20 of 2018 on Anti-Money Laundering and Countering the Financing of Terrorism;
- Federal Law No. (7) of 2014 on Combating Terrorism Offences;
- Cabinet Decision No. (10) of 2019 Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML-CFT Decision")
- Cabinet Resolution No. (24) of 2022 amending some provisions of Cabinet Resolution No. (10) of 2019 regarding the executive regulations of Federal Decree-Law No. (20) of 2018 regarding

countering money laundering crimes and combating the financing of terrorism and the financing of illegal organizations;

- Cabinet Decision No. (74) of 2020 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the suppression and combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions;
- Cabinet Decision No. (58) of 2020 regarding the Regulation of Beneficial Owner Procedure;
- Cabinet Resolution No. (53) of 2021 - Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Resolution No. (58) of 2020 Concerning the Regulation of Beneficial Owner Procedure;
- MOE Circular No. 2/2021-Guidelines for Designated Non-financial Business and Professions;
- Circular No. (2) of 2022 regarding Implementation of Targeted Financial Sanctions (TFS) on UNSCRs 1718 (2006) and 2231 (2015);
- Circular No. (4) of 2022 Interpretative Note on Assessing Jurisdictional Risk and the Consequential Application of AML/CFT Obligations in light of the United Arab Emirates being among the jurisdictions under increased monitoring by the FATF;
- MOE Circular No. 6/2021-Update on High-Risk Jurisdictions, jurisdictions under increased monitoring and identification of countermeasures to be applied by DNFBPs.
- Supplemental Guidance for Dealers in Precious Metals and Stones;
- Circular No. 08/AML/2021 dated 02nd June 2021 issued by Ministry of Economy, UAE
- FATF Recommendations; and
- Any other laws, regulations, notices, circulars issued by the Supervisory Authorities, National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations and The Financial Intelligence Unit in United Arab Emirates.

The AML Policy is derived from the laws and regulations of its local regulators Ministry of Economy of UAE and other regulatory and law enforcement bodies and also the AML/CFT international best practices.

10. COMPLIANCE OFFICER – DESIGNATION AND DUTIES

The company has designated a Compliance Officer for due compliance of its AML measures. He will act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions.

10.1 DUTIES OF COMPLIANCE OFFICER

The compliance officer appointed, have the appropriate competencies and experience and under his/her own responsibility, shall perform the following tasks:

- Detect Transactions relating to any Crime.
- Review, scrutinise and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.
- Review the internal rules and procedures relating to combating the Crime and their consistency with the Decretal-Law and the present Decision, assess the extent to which the institution is committed to the application of these rules and procedures, propose what is needed to update and develop these rules and procedures, prepare and submit semi-annual reports on these points to senior management, and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions.

- Prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organizations, and the means to combat them.
- Collaborate with the Supervisory Authority and FIU, provide them with all requested data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties.

10.2 ROLES AND RESPONSIBILITIES OF COMPLIANCE OFFICER:

- Ensure that appropriate policies, procedures, systems, and controls are established, developed, and maintained to monitor day-today operations for compliance with AML law, regulations, policies, procedures, systems, and controls.
- Conduct regular gap analysis on new notices/regulations/best practices issued by regulatory bodies vis-à-vis this AML & CFT Compliance policy.
- Conducting Enterprise-Wide AML/CFT Risk Assessment (at least on an annual basis).
- Conducting AML/CFT Risk Assessment of any new and/or modified product, service, and delivery channel
- Ensure adequacy of the systems and measures of customer due diligence and reasonability and creditability of the customer information obtained to establish a Business Relationship or carry out a transaction;
- Review high risk customers and ensure enhanced ongoing due diligence is undertaken for all high-risk customers / clients;
- Ensure to have in place a process for monitoring transactions for potential suspicion and reporting suspicious transactions;
- Control the level of the Company's compliance with the development of systems and procedures that ensure updating the records, and the extent to which such systems and procedures are applied on a regular basis;
- Ensure all key documents pertaining to KYC of customers, customer transactions, trainings and STR are retained for the minimum period of five (05) years.
- Arrange for AML/CFT training for all the employees; monitoring appropriateness and effectiveness of the AML/CFT training programs.
- Oversight on the implementation of AML policies, procedures, systems, and controls, including the risk-based approach to ML/FT risks.
- Filing STRs to the FIU, immediately once a suspicion is confirmed or maximum within two working days after completion of necessary investigation.
- Acting as focal or central point of contact between the FIU, the Regulator(s), and State authorities in relation to AML issues.
- Ensure prompt response to request for information by the FIU, Regulator(s), and State authorities in relation to AML issues.
- Producing bi-annual reports on the effectiveness of the AML / CFT controls, for consideration by senior management and Board.
- Exercising all other functions given to CO under AML/CFT Law, regulations or on issues relating to AML/CFT including accessing the GoAML portal of the FIU and filing STR and other reports to them.
- The CO must execute his responsibilities honestly, reasonably, and independently, particularly while receiving, investigating, and assessing internal STRs.
- Ensure that the Company sets the disciplinary regulations and procedures that ensure the commitment of that Company's employees to implementing the provisions of this policy.

11. INDEPENDENT AUDIT FUNCTION

The Internal Auditors functions as a third line of defense in AML & CFT compliance framework at the Company, first being business functions and second being the Compliance Department. The Company understands that internal audit is an integral part of the governance framework, thus the Company has outsourced the internal audit function to an external party and ensure that periodic assessment of effectiveness of the AML & CFT compliance program and present its findings and report the Owner.

12. CUSTOMER ACCEPTANCE POLICY

The Company shall follow the customer acceptance policy and procedures, in accordance with national and international regulations and best practices, to prevent the commencement of business relationships with customers against whom sanctions, or restrictions have been imposed, or with customers who pose a non-acceptable level of risk to the company and its business operations.

The Company will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate and shall establish AML/CFT procedures to assist and guide employees in carrying out their responsibilities and ensure that ML/FT risks are taken into consideration in the company's daily operations.

12.1 NATURAL AND LEGAL PERSON/ENTITY

The Company will establish the identity of its clients and beneficial owners prior to establishing business relationships with such persons and will take reasonable measures to verify identity when establishing a business relationship as noted below, subject to applicable EOCN requirements.

- **Natural Persons:** Identity will be verified to the company's satisfaction on the basis of official identity papers or other reliable, independent source documents, data, or information as may be appropriate under the circumstances as per the procedures mentioned in Know Your Customer (KYC) section of this Policy.
- **Corporations, Partnerships & other Legal Entities:** Identity will be verified on the basis of documentary evidence of due organization and existence as per the procedures mentioned in Know Your Customer (KYC) section of this Policy.

12.2 ULTIMATE BENEFICIAL OWNER

The Company will ensure to identify the identity of each beneficial owner who will be established and verified unless the identity is previously verified in accordance with the beneficial owner's role as a client. Identity will be verified to the Company's satisfaction on the basis of officially valid identity papers or other reliable, independent source documents, data, or information as may be appropriate and in the event verification, copies of such documents will be obtained.

12.3 POLITICALLY EXPOSED PERSONS

The Company shall only enter into a business relation with a PEP (natural person or legal person/ arrangements) upon gaining approval from the CO and the Owner during the onboarding phase. The Company will also ensure to conduct Enhanced Due diligence in line with their respective inherent risk involved and ensure that the customer whether a natural person or a legal entity is frequently monitored during the period of relationship.

Any declassification of PEP should be subject to an appropriate level of senior management review and approval. This review should be documented. Once a PEP has been de-classified, their prior PEP status should be noted for investigatory purposes (e.g., in the event of a suspicious activity reporting).

12.4 HIGH RISK JURISDICTION CUSTOMERS

The Company will ensure to undertake EDD process that is effective and proportionate to the ML/FT risks, including obtaining the approval of the CO, for establishing business relationships or one-off transactions with Customers from high-risk jurisdictions as per the procedures mentioned in this Policy.

12.5 OTHERS

The Company will ensure to undertake EDD process that is effective and proportionate to the ML/FT risks, including obtaining the approval of the CO and the Owner (if necessary), for establishing business relationships with third parties, NPO's or one-off transactions with Customers who conduct unusually complex transactions or those which have no clear economic or legal purpose and make sure to frequently monitor transactions processed by these customers and report to FIU in case of any suspiciousness.

12.6 PROHIBITED CUSTOMER TYPES/ BUSSINESS RELATIONSHIPS

The Company has categorized various kinds of clients whose commercial dealings call for increased levels of due diligence. This will often be the case in situations in which the company's business activities are anticipated to present a risk that is greater than the company's average risk. Transactions involving restricted customer categories are a type of ML/FT typology that is frequently employed by organizations that participate in the criminal underworld and professional money launderers.

The following are the conditions under which company, will refuse to accept a new business connection or will end an existing one. The following are some examples of such circumstances:

- Persons (natural or legal) who are unable to meet the company's identification and verification requirements or existing customers who no longer fulfil them.
- Shell banks / company
- Persons (natural or legal) or existing customers on sanction lists or lists provided by the EOCN or other regulatory authorities.
- Customers for whom suspicious transaction reports have been repeatedly submitted to the FIU, unless the latter requests the accounts to remain open so as to facilitate the investigation process.
- Prohibited transactions, these are transactions for which the company has assessed that the level of risk is not acceptable to the Company.

13. DUE DILIGENCE

- ❖ The Company has undertaken required CDD measures to verify the identity of the **Customer** and the **Beneficial Owner** before or during the establishment of the business relationship or before executing a transaction for a customer with whom there is no business relationship.
- ❖ And in the cases where there is a low crime risk, it will take necessary measures to complete verification of Customer identity after establishment of the business relationship, under the following conditions:

(a) The verification will be conducted in a timely manner as of the commencement of business relationship or the implementation of the transaction.
(b) The delay is necessary in order not to obstruct the natural course of business.
(c) The implementation of appropriate and effective measures to control the risks of the Crime.

- The Company has taken requisite measures to manage the risks in regard to the circumstances where Customers are able to benefit from the business relationship prior to completion of the verification process.

13.1 Customer On-boarding Process

13.2 CUSTOMER DUE DILIGENCE (CDD)

13.2.1 GENERAL REQUIREMENTS AND TIMING OF CDD

Customer Due Diligence (CDD) is the process of identifying and verifying the customer's identity, understand nature of business activities and establish purpose of business relationship before carrying out a transaction and/or establishing business relationship with customer. An adequate CDD / KYC process ensures that the Company deals with legitimate customers and prevents any possibility of financial crime risks.

Customer Due Diligence measures must be applied in below cases:

- Before establishing a business relationship
- Before carrying out a transaction for a customer with whom it does not have an established business relationship which value is equal to or greater than AED 55,000 for transactions carried out in a single transaction or multiple inter-related transactions.
- When there is a suspicion of money laundering or terrorism financing.
- When there are doubts concerning the veracity or adequacy of previously obtained identification documents and information.

13.2.2 CUSTOMER DUE DILIGENCE MEASURES

- Identify and verify the customer based on reliable, independent source documents, data and information issued by public authorities.
- Identify and verify beneficial owners of the business relationship and transactions.
- Identify and verify the identity of any person operating on behalf of the customer and seek proof of the authenticity.
- In case of legal arrangement, Trustees, managers, directors, or persons in equivalent positions; Settlors, founders, or persons in equivalent positions; The trust or legal arrangement, including any persons settling assets into the trust or legal arrangement; Protectors or persons in equivalent positions and exercising ultimate effective control over the trust; Beneficiaries or persons in equivalent positions; and Signatories.

- Understand the nature of business activities of the customer to ensure that funds used in the transaction are origin of legit sources.
- Collect specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, and/or infer the purpose and nature from the type of transactions or business relationship established.
- Background screening of the customer, Beneficial Owners, beneficiaries, or controlling persons, to screen for the applicability of targeted or other international financial sanctions, and, particularly in higher risk situations, to identify any potentially adverse information such as criminal history
- Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behavior.

13.2.3 CDD FOR INDIVIDUALS (IDENTIFICATION AND MEASURES)

Customer Identification for Transaction below AED 55,000

It is the policy of Company to identify customer/beneficial owner information for executing any transaction below AED 55,000. Below information must be identified for an individual customer:

- Name of the customer
- Nationality
- Date of Birth (DOB)
- Mobile Number
- Valid ID number
- ID Issue and Expiry Date

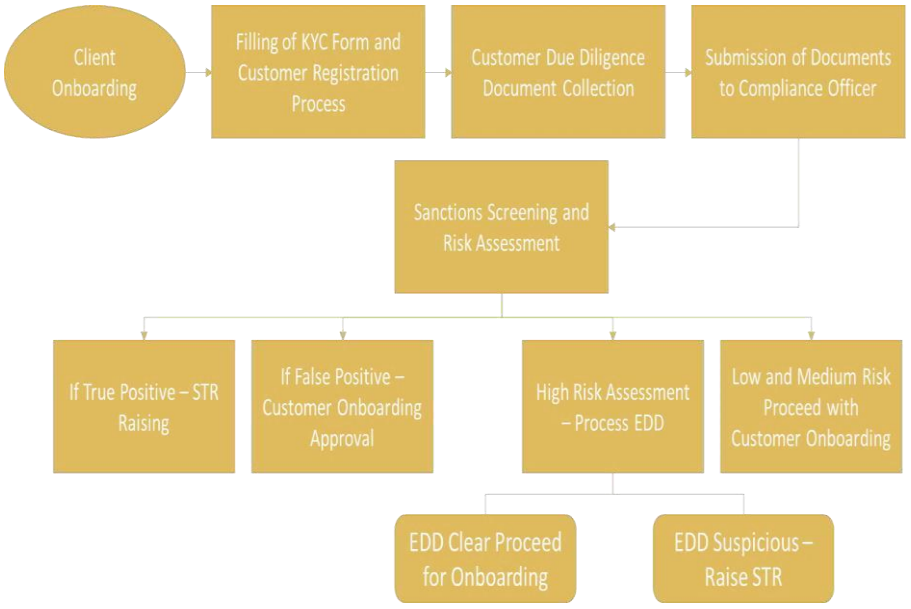
Customer Verification for Transactions below AED 55,000

A valid Identification document must be collected from the customer to verify above information.

Valid Identification document for individuals is:

- Emirates ID for residents
- Passport with valid visa for non-resident
- GCC identity card for GCC citizens

Customer Identification and Verification for Transactions above AED 55,000



Customer Identification

- Know Your Customer Form (Refer to KYC form for Individual)
- The minimum information to be obtained includes Name, Nationality, Date & Place of Birth, Occupation, Identification Number, Permanent Residential Address, Occupation, Employer Name and Employer Address.
- Nature and Purpose of Business Relationship
- Customer Verification
- Emirates ID for Emirati nationals and non-Emirati residents
- Passport and Valid Visa for non-residents
- GCC ID Card for GCC Citizens
- Address proof such as official document, utility bills, tax assessments, bank statements, insurance policies, or a letter from a public authority.
- The documents are required to be verified with original by the Company staff or apostille seal if country of issue is member of Hague Convention or concerned foreign embassy attestation (if not member of the Hague Convention).

13.2.4 CDD FOR LEGAL ENTITIES (IDENTIFICATION AND VERIFICATION MEASURES)

To apply CDD measures on Legal persons/ arrangements, below mentioned valid and official documents are collected:

- Know Your Customer Form (Refer to KYC form for Corporate)
- Minimum Legal Entity / Arrangement information such as Name, Legal Form, Registered Address, nature of business activities, ownership and/or control structure, Date and Place of Incorporation, Nature and Purpose of Relationship with the Company, Trade License / Commercial Registration Number, Identification details of shareholders, ultimate beneficial owner, authorized signatories, and senior management members etc.
- Commercial license issued by the Ministry of Commerce and Industry (for resident companies and establishments);
- For legal arrangements such as charities, trusts, etc., official identification documents attested by competent public authorities or bodies that issue these documents.
- In the case of non-resident companies and establishments, documents issued by competent authorities in the state in which they were incorporated or established.
- Identification documents of Ultimate Beneficial Owner or Controlling persons in case of legal arrangements.
- Authorization letter or Power of Attorney for Authorized Signatory/ Representative.
- Identification document of Authorized Signatory/Representative.
- Memorandum and Articles of Association.
- Address proof such as official document, utility bills, tax assessments, bank statements, or a letter from a public authority.

Identification of Ultimate Beneficial Owner

In case of legal person / arrangement, the Company identifies:

- The natural persons who ultimately have a controlling ownership interest of more than 25% either by shares or by voting rights in a legal person; or
- If there is doubt as to whether the persons with controlling ownership interest are indeed the beneficial owners, or where no natural person exerts control through ownership interests, the natural persons exercising control of the legal person through other means; or

- In the exceptional circumstances of an absence of any natural persons who have a controlling ownership or otherwise exercise effective control of the legal person, the natural person who holds the position of senior managing official.
- The Beneficial Owners may be verified by obtaining the Beneficial Information filed by the Legal Entity to the Registrar.
- The documents are required to be verified with original by the Company staff or apostelle seal if country of issue is member of Hague Convention or concerned foreign embassy attestation (if not member of the Hague Convention).

13.3 EXEMPTION TO CUSTOMER DUE DILIGENCE

The Company shall be exempted from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner, if such information is obtainable from reliable sources where the Customer or the owner holding the controlling interest are as follow:

- A company listed on a regulated stock exchange subject to disclosure requirements through any means that require adequate transparency requirements for the Beneficial Owner.
- A subsidiary whose majority shares or stocks are held by the shareholders of a holding company.

The listed Company (as defined above) should be subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In such case, the DPMS will obtain customer identification information from the stock exchange website, where it is listed.

13.4 ENHANCED DUE DILIGENCE (EDD)

The Company shall implement Enhanced Due Diligence measures in certain scenarios based on the high-risk factors.

The Risk factors can be categorized into four key areas:

- Customer Type Risk (such as Non-Resident Customers, Customer involved with high-risk business activities, non-profit organizations, PEP)
- Geography Risk (customers associated with or conducting transactions through High-Risk Countries)
- Product / Services/ Channel Risk (High risk products such as bullion trading / gold exchange/extraction/ refining etc.).
- Transaction Risk (cash, high value, and international transactions) - (Please refer to ANNEXURE II- High Risk Factors)

13.4.1 EDD MEASURES

EDD involves a more rigorous application of customer due diligence measures to be applied for high-risk business relationship. EDD measures may include, but not limited to:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources regarding customer identity.
- More detailed inquiry and evaluation of reasonableness about the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of each transaction.

- Perform adverse media checks on customer and/or beneficial owners to identify any involvement of financial crime.
- Update more regularly the information on customers and beneficial owners (at least annually).
- Obtain the approval of senior management to commence or continue the business relationship.
- Conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Payment to be carried out through an account in the customer's name with a financial institution subject to similar customer due diligence standards.
- Establish source of funds and purpose of transaction, if required obtain evidence also.

13.5 SIMPLIFIED DUE DILIGENCE

MAC & RO CAPITAL FZC under certain circumstances and in the absence of a ML/FT suspicion, is permitted to exercise simplified customer due diligence measures (SD) regarding customers identified as low risk through an adequate analysis of risks.

SDD generally involves a more lenient application of certain aspects of CDD measures, including elements as:

- A reduction in verification requirements regarding customer or Beneficial Owner identification;
- Fewer and less detailed inquiries regarding the purpose of the Business Relationship
- More limited supervision Of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information,

As per the AML Decision, SDD can be done in the following cases:

1. Identified low-risk customers
2. Listed Companies

13.6 SUPPLIER DUE DILIGENCE

13.6.1 OVERVIEW

Performing due diligence procedures on Suppliers reassures that the potential suppliers are financially and legally sound thus reducing the company's risk of exposure. The Company must ensure that all crucial information required to assess the supplier must be collected.

Suppliers could be either be outsourced for various products or services or could be third parties that provide essential commodities/ services. The SDD approach must be flexible and must emphasize on the main risk areas that the company is likely to be exposed to.

13.6.2 SUPPLIER DUE DILIGENCE MEASURES

Supplier Due Diligence involves (but not limited to) the following processes:

- Identifying and assessing supplier specific risks relative to the industry it operates;
- Screening for third party relationships of the supplier and therefore the regulatory environment;

- Identifying and screening third party connections which can expose the supplier to a greater risk of money laundering;
- Screening for any negative news that is against the supplier;
- Risk Assessment must be performed on all (trade related) suppliers and those classified as High Risk will be subject to Enhanced Due Diligence.
- As part of the Due Diligence process, vendors must be requested to fill a Know Your Supplier form prior to onboarding the supplier or executing transactions.

13.7 EMPOLYEE DUE DILIGENCE MEASURES

13.7.1 FIT AND PROPER CRITERIA

Human Resource Department when hiring employees, directors, board members and executive or supervisory management shall establish screening procedures to ensure that:

- Employees, directors, board members and executive or supervisory management, CO(s) and internal auditor(s) have the high level of competence necessary for performing their duties;
- Employees, directors, board members and executive or supervisory management, CO(s) and internal auditor(s) have appropriate ability and integrity to conduct the business activities of the Company;
- Potential conflicts of interests are taken into account, including the financial background of the employees, directors, board members, executive or supervisory management, CO(s) and internal auditor(s); and
- Persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the Company.

13.7.2 EMPLOYEE SCREENING

The screening procedures must include the following at a minimum:

- Initial screening of CVs.
- Verification of applicants' academic qualifications.
- Testing and interview.
- Employment history verification by contacting previous employers to confirm the employee's work experience and to gather information on previous role(s).
- Sanction checks must be applied on applicants before placing them in the employment.

13.8 NON-PROFIT ORGANISATIONS (NPO)

Non-Profit Organizations can often pose increased risks in regard to money laundering, the financing of terrorism, and the financing of illegal organizations. As part of an effective risk-based approach to AML/CFT, if the Company enters into or maintain Business Relationships with non-profit organizations (NPOs) it should take adequate EDD measures that are commensurate with the risks involved.

Examples of measures that supervised institutions should consider include, but are not limited to:

- Ensuring that the NPO is properly licensed or registered.

- Obtaining information about and assessing the adequacy of the NPO's AML/CFT policies, procedures, and controls;
- Obtaining sufficient information about the NPO's legal, regulatory, and supervisory status, including requirements relating to regulatory disclosure, accounting, financial reporting, and audit (especially where community/social or religious/cultural organizations are involved, and when those organizations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason);
- Obtaining sufficient information about the NPO's ownership and management structure (including taking into consideration the possibility of PEP involvement);
- The nature and scope of its activities;
- The nature of its donor base, as well as of that of the beneficiaries of its activities and programs; and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks;
- Performing thorough background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) on the NPO's key persons, such as senior management, branch or field managers, major donors, and major beneficiaries, to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information.

14. POLITICALLY EXPOSED PERSONS (PEP)

PEP is an acronym for Politically Exposed Persons. PEPs are persons with political power who can exercise political influence to carry out business activities and other administrative roles at their discretion. PEPs are most likely to be suspected of bribery and involved in corrupt activities, as they influence the spending of government funds. It is noteworthy that not only the person with the political power but also the family, friends, and close associates are also considered high-risk customers owing to the relationship they share with the PEP.

PEP's definition may differ from country to country, and it's a broad term in which businesses exercise their best judgment to identify a PEP. There are several factors that businesses need to consider in the risk assessment, such as the type of business, the country in which it operates, and the local AML regulations.

Identifying a Politically Exposed Person (PEP) can be a challenging task. The customer identification process is crucial as the exercise can help a business correctly assess the risk of creating a business relationship with PEP. If the identity and connections of the person are not known to the company and without correct risk assessment, mitigation of the risk becomes complex leading to reputational damage.

14.1 CATEGORIZATION OF PEPS

The definition of PEP differs from one country to another. People working in the government at different levels are described as PEPs.

- Members of Parliament, Heads of state – presidents, ministers, heads of departments, mayors, etc. can be categorized as PEP.
- People at the judicial levels, such as judges, are also classified as PEP. But not all judges fall under the PEP category.
- People holding diplomatic positions such as ambassadors and senior positions in the management of government-run organizations are also considered PEP.
- Bank officials in senior positions of national banks are regarded as PEPs.

- Senior officials in the sporting events responsible for organizing events and closing contracts on behalf of the government or ministry are also considered high-risk customers and fall under the PEP category.
- Parents, children, spouses, partners, siblings, and close relatives can also be termed PEPs. So, they are also subject to EDD because they are associated with PEP.
- People with close business relationships with PEP are also considered persons associated with PEPs; people holding joint beneficial ownership or legal arrangements with the PEP are considered high-risk customers. Associates who conduct transactions on behalf of the PEP are also categorized as high-risk customers. UBOs established to provide benefits to the PEP are also considered PEPs.

14.2 IDENTIFICATION OF PEPS

- **MAC & RO CAPITAL FZC** follows a robust AML compliance framework. Through this, can accurately assess the risk of different customers. It helps to correctly identify and verify the customer's identity and flag the potential PEP – whether domestic PEPs, foreign PEP or HIOs.
- **MAC & RO CAPITAL FZC** relies on AML screening software, which helps the company to identify and verify customers and their status as PEP or associated with PEP.
- With CDD and EDD processes and continuous monitoring, the company accurately identify PEPs, monitor their status, and transaction with them.
- **MAC & RO CAPITAL FZC** identifies the PEP at the first step of initiating the customer relationship. Also, continuous monitoring is applied, as the PEP status may change over a while.
- It keeps a tab on the PEP status. It helps to assess the risk involved during the customer journey correctly. To assess the PEP status accurately, it tries to get accurate information in real-time.
- PEPs are entrusted with administration responsibilities and wield power to get things done at their discretion. Therefore, **MAC & RO CAPITAL FZC** uses EDD as a powerful method to identify the source of PEP's funds and verify their financial and professional background before becoming a PEP.
- EDD will help make an informed decision regarding establishing a business relationship with people identified as PEPs – they may be close associates, family, or friends of the PEP. Continuous monitoring of the customer profile is also required to detect any changes from the original verification conducted at the time of on-boarding. Often non-profit organizations, charities, etc., are misused to launder money by the PEPs, so the company also verifies the PEPs' connection with such charitable organizations.

15. CASH ACCEPTANCE PROCEDURES

UAE's ML/FT national risk assessment has pointed out that use of cash is prevalent in transactions especially in gold and precious metals segments. To mitigate the risk related to cash handling, the Company has implemented this point in the AMLCFT policy. This is required to implement and maintain the smooth operational activity for staffs, create staff awareness with the operational guidelines, procedure and practice for handling cash and ensure fast and accurate service to our valued customer.

Cash handling policy is a set of rules on how to manage cash on behalf of the company. This policy mandates maker checker for cash handling. Cash transactions will be checked and tallied on a daily basis.

As part of the Standard Operations Procedures, the company follows below appended steps in order to record the transaction as part of the due diligence procedures:

a) Cashier/Sales Representative must collect and verify the original identification document at the time of creating customer account in the system.
b) A copy of the original identification documents must be certified with the stamp "original seen and verified" by the verifier employee along with his name, title and date.
c) Copy of the identification document is collected and attached with the Sales Invoice and keep them in the store area.

Upon receiving the cash for transactions, there are some proper cash-handling procedures that the company follow:

Reconciliation: A manager counts the cash collected within a certain period, typically one business day. They ensure that cash receipts and deposits match.

Security: Employees store cash in a secure location during and after business hours and during transportation to the bank.

Separation of Duties: There are clearly defined roles for managing each part of the cash handling process from reconciling regularly to depositing cash in the bank.

Documentation: Another manager is in charge of accounting for all cash transactions.

15.1 Roles and Responsibilities for Cash Handling Staff

Depending upon staff availability functions given below may be followed by the same staff member or allocated to different persons.

Front-end Staff

Description of Role

- Create and send invoices.
- Record sales as appropriate.
- Update the system.

Cashier

Description of Role

- Conduct cash transactions with customers
- Provide a receipt to customer paying in person.
- Enter transactions into accounts receivable system
- Count the cash and submit the cash & supporting documentation to the Supervisor at the end of their shift.

Supervisor

Description of Role

- Monitor cash receipting functions.
- Authorize various transactions, such as refunds, voids, and cash drawer reconciliations.
- Store the cash in a secure location until it is deposited.
- Deliver deposit to the bank or designated deposit drop location.

Accountant

- Verify that the Cashier has deposited all cash received.
- Conduct Reconciliation of all cash accounts

15.2 Controls Implementations

Following controls have been placed by **MAC & RO CAPITAL FZC L.L.C**:

1. For loss prevention, having designated roles for counting and depositing cash reduces discrepancies and limits how many hands are touching the money.
2. We have installed CCTV cameras that help deter and catch criminals. Furthermore, we have Point-of-Sale (POS) system to securely store money and prevent internal and external theft.
3. We are using an armored delivery service that reduce the amount of time that employees are off-site.
4. Distinguish Cash Management Roles

Reconciliation: This role involves handling cash register reconciliation at the end of each business day for each POS cash register.

15.3 Due Diligence for Cash Transactions

Receipts in Cash

Cash receipts above AED 55,000 for single transactions or linked transactions should be supported with evidence of source. We should understand customer's profession/ business activities declared in KYC form and determine if the customer's source of fund is legitimate. In case, we have suspicion about declared information, you request the customer to provide bank statement, or an ATM/cheque withdrawal slip or foreign currency exchange receipt (for tourists) which can show corresponding withdrawal in the same amount as of transaction.

Where transaction amount exceeds AED 55,000 in cash following procedure is maintained as part of the Due Diligence Process:

a) KYC form is kept at the store which employees should request the customer to fill in.
b) Information furnished by the customer shall be verified with the identification document collected.
c) SDD is applied for the customer resident in UAE and transaction amount is less than AED 20,000 whether paid in cash/any other mode.
d) As part of CDD measures, employees are required to:
   - Verify the identity of the customer.
   - Obtain a duly filled KYC form from customer.
   - Obtain satisfactory evidence for the source of funds.

15.4 Reporting

Under the AML-CFT Law and Article 3 (2) of the AML-CFT Decision, Dealers in Precious Metals and Stones are obliged to apply the required AML/CFT measures when they qualify as DNFBP. This occurs whenever they carry out any single transaction, or several transactions that appear to be interrelated whose monetary value equals or exceeds AED 55,000. The transaction has to be reported in DPMSR in the go AML Portal. The same has been covered in Section 7.2 of the AML CFT Policy and Procedures 2023.

16. KNOW YOUR EMPLOYEE (KYE)

Know Your Employee policy should be conducted have the following stages.

a. Pre- Employment Stage
b. Course of employment
c. Employee Conduct

16.1 Pre – Employment Stage:

Due diligence in KYE starts at the recruitment stage, to know if the promising candidates are telling the truth. At the initial stage references should be checked; a reference check can be done by the organization or by outsourced agencies. References of a prospective employee - You can verify if there is any criminal conviction; this can be achieved by getting:

- A police clearance certificate from the police station of the last known residences.
- The relieving letter from the previous employer is taken.
- The past employer can be asked to provide few details like; did they really work for that company stated on the CV? Employment credentials such as designation, role, compensation, conduct and reason for leaving will be ascertained.
- How was their conduct of the prospective employee?
- References provided by the prospective employee can be requested to provide information which the prospective employee has stated on the resume' or job application.
- The references given by the candidate shall be contacted & affirmed. (First degree relations should not be hired)
- In case the verification or background check services are provided by a vendor, Company must ensure the standards & procedures the organization applies while conducting the check. Are their standards comparable to yours? Are there procedures reviewed by an independent firm.
- Screening of Employee names against the sanctions list.

16.2 Course of Employment:

Even though the reference checks have been applied, it is advisable to have random checks to ensure that the employee maintains its responsibility to be a trustee of the organization. It is good management practice to monitor your employees' performance and understand what makes them stick, but this routine procedure can also unearth internal threats to your business.

16.3 Employee Conduct:

Signs which could raise a signal for verifying the employees conduct and behavior: -

- **Staff Behavior**: A change in the employee's lifestyle, especially when the spending etc. by an employee sees a drastic change then what an employee at the same level could afford.
- **Credit cards/Loans**: the employees availing frequent loans and credit cards should pose a question for the employer. Too many approvals and NOCs provided to employees can not only lead to defaults but can also cause the organization to be blacklisted for getting further benefits from banks etc.

- **Overzealous nature and relation with select customers**: There could be possibilities of Customers offering bribes and commissions to employees for conducting frauds, embezzlements and money laundering, Frequent checks, and controls on the activities of employees can help detect these activities at an early stage.
- **Timing:** Many a times employees employed in critical areas of operations and accounts have been caught for internal frauds etc. These employees have been reported to have long working hours, coming early before the time to office and sitting till late in office.
- **Compromising on data & system integrity**: employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely for mitigating any risk of fraud.

17. TRAINING AND AWARENESS

17.1 OVERVIEW

In order for the ML/FT risk assessment and mitigation measures to be effective, the Company shall ensure that its employees have a clear understanding of the risks involved and can exercise sound judgment, both when adhering to the organization's ML/FT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/FT risk, the Company shall ensure that its employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks.

17.2 EMPLOYEE'S TRAINING

MAC & RO CAPITAL FZC has an ongoing employee training under the leadership of the Compliance Officer.

The AML/CFT training materials prepared by the Company will cover at least the following topics. These topics should be covered in greater depth, and additional topics should be covered as appropriate, on a risk sensitive basis depending on the role of each employee:

- Overview AML/CFT, definitions, typologies as well as contemporary trends.
- ML/FT risks associated with the products and services offered.
- AML/CFT policies and procedures including the highlights on recent changes.
- The regulatory responsibilities and obligations of employees under AML/CFT Laws, Regulations, Notices, and the Standards.
- Description of Know Your Customer process and its importance.
- Due Diligence measures and procedures for monitoring transactions.
- Sanction screening and PEP screening procedures.
- Red flags to identify unusual transactions or transaction patterns or customer behaviors.
- Processes and procedures of making internal disclosures of unusual transactions.
- Roles of the CO and the Senior Management.
- Awareness on Tipping off.
- Record retention policy.
- Reference to industry guidance and other sources of information.
- Emerging ML/FT risks and measures to mitigate such risks.
- Penalties for non-compliance with the AML/CFT Laws, Regulations, Notices, and the Standards; and
- Disciplinary procedures to be applied on employees for not adhering to the AML policy and procedures.

Means of the training may include educational pamphlets, videos, internet systems, in-person lectures, and explanatory memos. The operations are reviewed periodically to see if certain employees, such as those in compliance, margin, and corporate security, require additional specialized training.

17.3 ANNUAL TRAINING PLAN

The **MAC & RO CAPITAL FZC** shall ensure that AML/CFT trainings are conducted at all levels within the Company (including functional heads, Senior Managements and Owner). To achieve this goal, the CO will develop an annual training plan after assessing employees specific training needs and their respective obligations at the beginning of the year.

All employees must be trained to understand how to comply with the legal and regulatory framework in the UAE and abide by the Company's policies and procedures. It is not acceptable for an untrained employee to have responsibility for collecting or disbursing customer funds and initiating transactions.

The Company shall provide AML/CFT training as follows:

- **Induction Training:** All the new joiners shall be provided with the AML training as soon as reasonably practicable within 30 days after joining the firm and respectively new joiners is not allowed to serve the any customer independently until attending the training.
- **Refresher Training:** Refresher trainings shall be provided by an external party at regular intervals as per the annual training plan of the Company. The Company may determine the frequency of refresher training based on the risk exposure of the employee. However, employees who deal directly with customers, products and services will receive annual training at a minimum.
- **Ad-hoc Training:** Additional training will also be provided by the Company on ad-hoc basis as and when required (whenever there are changes in the AML Laws, Regulations, Notices, or the Company's AML policy/procedures).

17.4 ASSESSMENT CRITERIA

For Employees who score less than 70% of the total score in the assessment tests followed by the training shall be given a residual training within a period of 30 days and an assessment will be conducted following the same, if the employee fails to pass the residual training for 3 times the matter will be escalated to Senior management for the necessary disciplinary action.

17.5 CIRCULATION OF AML/CFT POLICY

The CO shall ensure that all the staff are provided with a copy of the AML/CFT Policy and are well educated and trained in compliance of the AML/CFT policy. The CO must provide to all the employees with approved AML policy upon joining for their acknowledgement and obtain an undertaking letter from them declaring that they fully have read and understood the AML Policy and will comply and establish with the same.

18. CUSTOMER EXIT POLICY

1.1 TERMINATION BY LAW

- When the Company has received court order in respect to an existing or registered customer,
- At the time when the Company has to comply with EOCN, FIU or other equivalent regulatory requests,

- When the Company has to act in accordance with the instruction of UAE police department,
- Any other matters to meet the provisions under law.

1.2 SANCTION LIST

- When the customer is listed in Money Laundering or Terrorism Financing.
- When the customer is identified as he/she has involved in severe crime like Human Trafficking, Smuggling, Narcotic dealing, Tax evasion, corruption etc.
- The individual/entity is listed in sanction list of EOCN, MENAFATF, OFAC, UN or other similar organization.
- When the customer is identified as PEP, but the final decision of termination is limited to BOD approval.
- Any other matters impending under sanction list.

1.3 OTHERS

- When the customer has conducted fraudulent attempt/activities.
- Mutual agreement
- Or any event that is under violation, unethical or subject to closure of client relationship to secure the reputation of the Company and to comply with regulatory laws.

If the Company encounter with any situation mentioned above, it will consider exiting relationship with customers and also committed to report the incidents to regulatory organization. Additionally, input the names in Internal Blacklist master to assure the Client Exit process.

2. RECORD RETENTION

2.1 OBJECTIVE

The objective of record keeping is to ensure that the Company shall be able to provide the information about the customer and to reconstruct the transactions undertaken at the request of the relevant authorities at any given time. With reference to Paragraph 3.4 of the Guidance Note, record retention includes electronic communication and documentation as well as physical, hard copy communication and documentation may be by way of original documents, stored or in computerized form whichever is suitable.

2.2 RECORD RETENTION GUIDELINES

- All documents/records related to transactions such as transaction receipts, Source of Fund, KYC, Customer Due Diligence and Enhanced Due Diligence must be retained for a minimum period of five (5) years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the Company has been carried out.
- AML training registers, training plans, AML training materials and other evidence for providing AML training must be retained for a period of five (5) years from the date of training.
- Supporting documents for the transaction monitoring and investigations carried out on unusual transactions must be retained for a minimum period of five (5) years.
- Copies of transaction reports sent and related documents for at least five (5) years after the date the report was made to the Centre.
- The risk assessment and any underlying information for a period of five (5) years from the date the assessment was carried out or updated.

- All documents related to STRs including internal disclosures by employees must be retained for a minimum period of five (5) years from the date the STR was reported.
- In situations where the records relate to on-going investigations, or transactions that have been the subject of a disclosure, they should be retained for a minimum period of five (5) years from the date the case was closed.
- Any other records to demonstrate compliance with the AML/CFT Laws, Regulations, Notices, and the Standards must also be retained for a minimum period of five (5) years.

Additional guidelines: -

- Records include electronic communication and documentation as well as physical, hard copy communication and documentation.
- Retention may be by way of original documents (i.e., hard copies), stored on microfilm or in electronic form (i.e., soft copies).
- Records must be sufficient to permit the reconstruction of individual transactions and provide details of the parties at the request of the relevant authorities.
- Records must be made available to the relevant authorities as and when requested.

2.3 REQUIRED RECORD TYPES

MAC & RO CAPITAL FZC retains records which can be classified broadly into the following categories:

1. Transaction Records — This category relates to operational and statistical records, documents and information concerning all (commercial or financial) transactions executed or processed by the Company, whether domestic or international in nature.

2. CDD Records - This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:
    - Customer Information, including account files and business correspondence, and results of any analysis undertaken;
    - Company Information;
    - Reliance on Third Parties to Undertake CDD
    - Ongoing Monitoring of Business Relationships
    - Suspicious Transaction Reports (STRs)

3. RULES BASED TRANSACTION ONGOING MONITORING PROCEDURE

3.1 TRANSACTION MONITORING

The Company shall undertake CDD ongoing supervision of business relationships, including reviewing transactions that are carried out throughout the period of the business relationship, to ensure that the transactions conducted are consistent with the information they have about Customer, their type of activity and the risks they pose, including - where necessary - the source of funds.

Following a risk-based approach, the Company shall scrutinize customers' transactions to ensure that such transactions are in line with the customer profile, source of fund, and in high-risk cases, the source of customer's wealth.

Under some circumstances (for example, in the case of ongoing business relationships with suppliers or customers), the Company may be in a position to monitor the status and activity of the business relationship over time. However, in other situations (such as those involving occasional or one-off customer transactions), it may not always be possible for the Company to perform detailed ongoing monitoring of the entirety of their business partners' or customers' activity.

It is important that the Company take reasonable steps to protect themselves from misuse by criminals and terrorists. Particularly in circumstances in which high-risk customers have been identified, DPMS should make reasonable efforts to monitor activity related to the transactions, services, or customer activities with which they are involved.

3.2 UPDATION OF CDD INFORMATION AND DOCUMENTS

The Company shall undertake CDD measures and ongoing supervision of business relationships, including ensuring that the documents, data, or information obtained under CDD Measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories.

The CO shall conduct periodic review of customer information, particularly for high-risk customers and transactions, to ensure that documents are valid and relevant.

Such reviews shall take place at least:

- For Low Risk Profile Clients – once every 3 years;
- For Medium Risk Profile Clients – once every 2 years;
- For High Risk Profile Clients – once every 1 year.

4. INTERNAL AUDIT

Internal Audit shall ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. **MAC & RO CAPITAL FZC** confirms to have in place an independent audit function to test the effectiveness and adequacy of their internal polices controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations. The scope of such audits should include but not be limited to:

- Examine the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements,
- Assess training adequacy, including its comprehensiveness, accuracy of materials training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual

or suspicious activity from all business lines to the personnel responsible for investigating unusual activity.

5. REPORTING TO FINANCIAL INTELLIGENCE UNIT (FIU)

5.1 ABOUT FIU

The core function of the FIU is to conduct operational analysis on STRs, and information received from FIs, other companies as well as from Competent Authorities, and to support the investigations of Law Enforcement Authorities. It does so by identifying specific targets (such as persons, funds, or criminal networks) and by following the trail of specific transactions in order to determine the linkages between those targets and the possible proceeds of crime, money laundering, predicate offences, and terrorist financing.

5.2 SUSPICIOUS TRANSACTION REPORT/ SUSPICIOUS ACTIVITY REPORT (STR/SAR)

Any suspicious transactions or activities that do not include confirmed or potential matches to the UAE Local Terrorist List or UN Consolidated List should be reported to the FIU by raising a STR/SAR through the go AML platform.

The Company will ensure to file any the Suspicious Transaction Reports / Suspicious Activity Reports on the Go AML portal upon receipt of any I STR' s received from the FLA's and scrutinization of the said cases by the Compliance Department.

5.3 DEALERS IN PRECIOUS METALS & STONES REPORT (DPMSR)

- All **Cash transactions** with individuals equal or exceeding AED 55000.00 need to be reported in the GoAML System.
- Exceptions: (Not to Report) – Any Credit Card /Cheque or Bank Transfer transactions of any amount. Only if Suspicious then to be reported through STR Option in GoAML System.

- All Cash/ International Wire Transfers / Transfers through Exchange Houses or Remittance Companies equal or exceeding AED 55000.00 need to be reported in the GoAML System.
- All Settlements in USD with following qualifications.
- Both Entities having accounts in UAE and transfers done for USD payments.
- USD Settlements done between two Free zones Within UAE, having different bank accounts, and Settlements between Free zone and onshore companies registered in the UAE.

5.3.1 EXCEPTIONS: (NOT TO REPORT)

- AED Settlement where both the parties have accounts in same bank in the UAE.
- AED Settlement where both the parties have accounts in different banks in the UAE.

- USD Settlement where both the parties have accounts in same bank in the UAE.
- Trade between related parties Mainland to Free zone having same bank account transactions and Vice Versa.
- Barter transaction (Exchange of Gold)
- Intra Company Transactions
- Transaction not routed through the UAE Bank Account.

5.4 HIGH RISK JURISDICTION TRANSACTIONS REPORTING

Business relationship or transactions involving natural person or legal entities from high-risk jurisdictions must be reported to Financial Intelligence Unit (FIU) by CO (through the Go AML Portal).

Such reported transactions may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.

The obligation for reporting as well as putting on hold is for cross border transactions through banking or remittance channels. It includes transactions which originate from, are destined to, or are routed through the High-Risk Jurisdictions.

The transactions also include cross border transactions from/to any country where the remitter or the beneficiary is individual or legal entity associated with high-risk jurisdictions. Individuals are associated with High-Risk Jurisdictions by virtue of Nationality or Residence. Legal Entities are associated with High-Risk Jurisdiction by virtue of its Place of Incorporation or if it is controlled by or its authorized signatory is an Individual from the High-Risk Jurisdiction.

5.5 FUND FREEZE REPORTS

In case a confirmed match is identified, the reporting entity must freeze without delay (within 24hrs) all funds and other assets and submit a FRR through go AML within five business days of implementing the freezing measures, along with all the necessary information and documents regarding the confirmed match and the freezing measures taken.

The Company will ensure to file any Fund Freeze Reports, if necessary, in the Go AML portal upon receipt and scrutinization of any confirmed match by the Compliance Department.

5.6 PARTIAL NAME MATCH REPORT (PNMR)

In case a potential/partial name match is identified, the reporting entity is required to suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a Partial Name Match Report (PNMR) through goAML, along with all the necessary information and documents regarding the name match are submitted and maintain suspension measures related to the potential match until further instructions are received from Executive Office via goAML on whether to cancel the suspension (‘false positive’) or implement freezing measures (‘confirmed match’).

The Company will ensure to file any Partial Name Match Reports, if necessary, in the GoAML portal upon receipt and scrutinization of any partial name match by the Compliance Department.

5.7 INFORMATION REQUEST FRON FIU (RFI)

As part of its obligations to comply with anti-money laundering and counter-terrorism financing regulations, the Company may receive information requests from the FIU (Financial Intelligence Unit).

In such cases, the Company must ensure that it responds to these requests in a timely and accurate manner.

6. CONFIDENTIAL REPORTING OF AML NON – COMPLIANCE

The Managers, officials or staff, will not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard.

7. BI – ANNUAL COMPLIANCE REPORTS

The CO shall prepare and present bi-annual report on AML/CFT Compliance Function in order to assess the effectiveness of the AML/CFT policies, procedures, systems, and controls to prevent M//TF.

The Bi-Annual Compliance Reports must be submitted within one (1) month from the end of each reporting period to the Owner for his review and approval.

Such report shall include, but not limited to: -

- Assessment of ML/FT risks associated with the business and the effectiveness of its policies, procedures, systems, and controls.
- Summary of the gap analysis between the AML/CFT Program and existing AML Laws, Regulations, Notices, and the Guidelines as well as the actions taken by the CO to bridge or resolve such gaps.
- The number of internal suspicious disclosures made by employees and the number of cases investigated, closed, kept open for future monitoring, or reported to the FIU as STRs during the reporting period.
- The number of suspicious transactions detected and reported to the FIU via independent transaction monitoring by the CO during the reporting period.
- Changes in the AML/CFT policies and procedures reviewed and the details of any AML/CFT policy or procedures newly introduced during the reporting period.
- Statistics on total employees, new joiners during the reporting period, number of employees trained, and the number of employees not trained (if any) including reasons for not training employees.
- Recommendations to the Owner for the improvement of the AML/CFT function.
- Details of CO's requests for additional human resources, systems, controls, tools, and technology changes for the attention of the Owner.
- The conclusion of the CO about the effectiveness of the existing AML/CFT function.

8. NO RETALIATION POLICY

The Company is committed to maintaining a culture of compliance with all applicable anti-money laundering (AML) and countering the financing of terrorism (CFT) laws, regulations, and policies. As part of this commitment, the Company strictly prohibits any form of retaliation against employees who report any concerns or suspected violations of AML/CFT regulations, policies, or procedures.

The Company values and encourages the reporting of any such concerns, and will not tolerate any form of retaliation, including but not limited to, termination, demotion, denial of promotion or training, or any adverse employment action against employees who report any AML/CFT concerns in good faith. As a result of their good faith performance of their statutory obligations to comply with this Policy, all employees and authorized representatives are protected by the relevant articles of the AML & CFT Law and AML & CFT Decision from any administrative, civil or criminal liability.

Any employee who believes that they have been retaliated against for reporting any AML/CFT concerns is encouraged to report the matter immediately to their supervisor, or to the CO. The Company will investigate all such reports promptly, thoroughly, and confidentially, and will take appropriate remedial action, up to and including disciplinary action, against any employee found to have retaliated against another employee for reporting any AML/CFT concerns.

9. REVIEW

The Company conducts a periodic review of the policy. In case of amendment in statutory provisions/ regulations necessitating amendment, the relevant portions of policy shall be deemed to have been modified from the date of amendment in relevant statutory provisions. In such case, the modified policy shall be placed for review by the Board in regular course.

A regular review of the "Compliance Manual" shall be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources and should be accompanied by a formal assessment or written report. If and when regulations are amended concerning reporting of suspicious activities, **MAC & RO CAPITAL FZC** will amend the Compliance Manual to comply with those regulations.

Scope:

- Examine the adequacy of CDD policies, procedures, and processes, and whether they comply with internal requirements.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers, and geographic locations) on sample testing basis.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program if any.
- Reviewing policies, procedures, and processes for suspicious activity monitoring.
- Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.
- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel or department responsible for evaluating unusual activity.
- Assess the adequacy of recordkeeping.

10. COMMUNICATION

The Compliance Officer shall ensure that this policy is communicated to all management and relevant staff including Customers and all concerned.

11. NON – COMPLIANCES PENALTIES UNDER THE RESPECTIVE LAWS

- Article (22-1) - Any person who commits or attempts to commit any of the acts set forth in Clause (1) of Article 2 of this Decree-Law shall be sentenced to imprisonment for a period not exceeding ten years and to a fine of no less than (100,000) AED one hundred thousand and not exceeding (5,000,000) AED five Million or either one of these two penalties.
- A temporary imprisonment and a fine of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) shall be applied if the perpetrator of a money laundering crime commits any of the following acts:
  - *If he abuses his influence or the power granted to him by his profession or professional activities.*
  - *If the crime is committed through a non-profit organization.*
  - *If the crime is committed through an organized crime group.*
  - *In case of Recidivism*.
- Article (22-2) - An attempt to commit a money laundering offense shall be punishable by the full penalty prescribed for it
- Article (22-3) - A life imprisonment sanction or temporary imprisonment of no less than (10) ten years and penalty of no less than AED 300,000 (three hundred thousand dirham) and no more than AED 10,000,000 (ten million dirham) is applied to anyone who uses Proceeds for terrorist financing.
- Article (22-4) - A temporary imprisonment sanction and a penalty of no less than AED 300,000 (three hundred thousand dirham) shall be applicable to anyone who uses the Proceeds in financing illegal organizations.
- Article (22-5)- The Court may commute or exempt from the sentence imposed on the offenders if they provide the judicial or administrative authorities with information relating to any of the offenses punishable in this article, when this leads to the disclosure, prosecution, or arrest of the perpetrators.
- Article (23-1) - A penalty of no less than AED 500,000 (five hundred thousand) and no more than AED 50,000,000 (fifty million dirham) shall apply to any legal person whose representatives or managers, or agents commit for its account or its name any of the crimes mentioned in Federal Decree-Law No (20) of 2018.
- Article (23-2) - If the legal person is convicted with terrorism financing crime, the court will order its dissolution and closure of its offices where its activity is performed.
- Article (23-3) - Upon issuance of the indictment, the court shall order the publishing of a summary of the judgment by the appropriate means at the expense of condemned party.
- Article (24) - Imprisonment and a fine of no less than AED 100,000 (one hundred thousand) and no more than AED 1,000,000 (one million dirham) or any of those two sanctions is applied to anyone who violates on purpose or by gross negligence the provision Article (15) of the Federal Decree Law No (20) of 2018.

- Article (25) - Imprisonment for no less than six months and a penalty of no less than AED 100,000 (one hundred thousand dirham) and no more than AED 500,000 (five hundred thousand dirham) or any of these two sanctions shall apply to anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the Competent Authorities.
- Article (25) bis - Imprisonment for no less than three months and a penalty of no less than AED 50,000 (fifty thousand dirham) or any of these two sanctions shall apply to whoever possesses, conceals, or performs any operation of funds when there is sufficient evidence or presumption of illegality of its source.
- Article (26) bis - Imprisonment for no less than six months and a penalty of no less than AED 200,000 (two hundred thousand dirham) and no more than AED 5,000,000 (five million dirham) or any of these two sanctions shall apply to anyone who violates the provision of Article 16 bis of this Decree Law.
- Article (28) - Imprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the Competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions.
- Article (31) - Imprisonment or a fine of no less than AED 10,000 (ten thousand dirhams) and no more than AED 100,000 (one hundred thousand dirhams) shall be applied to any person who violates any other provision of the Federal Decree-Law No. (20) of 2018.

12. DISCLAIMER

- Any employee who has reasons to believe that **MAC & RO CAPITAL FZC** might be or has been exposed to funds from a doubtful source should come forward to management immediately.
- Any employee who is found in violation of the terms of this Policy will be subject to disciplinary action.
- Any employee with direct knowledge of potential or apparent violations of this Policy who fails to report such acts to Company management will also be subject to disciplinary action.
- Any employee who knowingly misleads or hinders an investigation to reported violations of the Policy and any relevant and applicable law also may be subject to disciplinary action.
- Disciplinary actions may risk termination of employment. The same applies to third parties that are associated with **MAC & RO CAPITAL FZ C**ooperation's. Third-parties risk having their contracts re-evaluated or terminated.

13. ANNEXURE – I GLOSSARY

AML	Anti-Money Laundering
CBUAE	Central Bank Of UAE
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
CO	Compliance Officer
CP	Customer Profile
DNFBPs	Designated Non-Financial Business and Professions
DPMS	Dealers in Precious Metal and Stones
EDD	Enhanced Due Diligence
EOCN	Executive Office for Control and Non-Proliferation
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FPEP	Foreign Politically Exposed Person
KYC	Know Your Customer
CO	Money Laundering Reporting Officer
MENAFATF	Middle East and North Africa FATF
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PF	Proliferation of Funds
PMS	Precious Metal and Stones
RBA	Risk Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
UBO	Ultimate Beneficial Owners
UN	United Nations
WMD	Weapons and Mass Destruction

14. ANNEXURE – II DEFINITIONS

AML / CFT	Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Beneficial owner	The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client; or the natural person on whose behalf a transaction is being conducted; or the natural person who exercises effective ultimate control over a legal person or legal arrangement.
Business Relationship	Any ongoing commercial or financial relationship established between financial institutions, designated non-financial businesses and professions, and their customers in relation to activities or services provided by them.
Client /Customer	Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law with one of the financial institutions or designated nonfinancial businesses and professions.
Competent Authorities	The competent government authorities in the State entrusted with the implementation of any provision of this Decree Law
Confiscation	Permanent expropriation of private funds or proceeds or instrumentalities by an injunction issued by a competent court.
Controlled Delivery	The process by which a competent authority allows the entering or transferring of illegal or suspicious funds or crime revenues to and from the UAE for the purpose of investigating a crime or identifying the identity of its perpetrators.
Crime	Money laundering crime and related predicate offences, or financing of terrorism or illegal organizations.
Customer Due Diligence (CDD)	The process of identifying or verifying the information of a client or Beneficial owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it for the purpose of this Decree-Law and its Implementing Regulation.
Decree- Law	Federal Decretal-Law No. (20) of 2018 on Anti- Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Designated Non-financial Businesses & Professions	Anyone who conducts one or several of the commercial or professional activities defined in the Cabinet Decision No.10 of 2019
Financial institutions	Anyone who conducts one or several of the activities or operations defined in the Implementing Regulation of the present Decree Law for the account of /or on behalf of a client.
Financing Illegal Organizations	Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or its members.
Financing of Terrorism	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014
Freezing or seizure	Temporary attachment over the moving, conversion, transfer, replacement or disposition of funds in any form, by an order issued by a competent authority.

Funds	Assets in whatever form, tangible, or intangible, movable or immovable including national currency, foreign currencies, documents, or notes evidencing the ownership of those assets or Associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.
High Risk Customer	A Customer who represents a risk either in person, activity, business relationship, nature of geographical area, such as a Customer from a high-risk country or non-resident in a country in which he does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by financial institutions, or designated non-financial businesses and professions, or the Supervisory Authority.
Illegal Organizations	Organizations whose establishment is criminalized, or which exercise a criminalized activity
Law-enforcement Authorities	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidence on the crimes including AML/CFT crimes and financing illegal organizations
Legal Arrangement	A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as trust funds or other similar arrangements.
Legal person	Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.
Local Terrorist List	Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) Paragraph (I) of Federal Law No. (7) of 2014 on Combating Terrorism Offences.
Means	Any means used or intended to be used to commit an offence or felony.
Money Laundering	Any of the acts mentioned in Clause (1) of Article (2) of the present Decree-Law
Non-Profit Organizations	Any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit legal arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities.
Politically Exposed Persons (PEPs)	Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organizations or any prominent function within such an organizations; and the definition also includes the following

	1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include (a) Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP. (b) Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.
Predicate Offence	Any act constituting an offense or mis demeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries
Proceeds	Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
Purpose of transaction	An explanation about why a customer is conducting a transaction or the reason for which the funds will be used. Examples of purpose of transaction are - family support, education, medical, tourism, debt settlement, financial investment, direct investment, or trading etc. For verification of the purpose of transaction, documents may include any documentation proving the purpose for which the money will be used.
Registrar	The entity in charge of supervising the register of commercial names for all types of establishments registered in the UAE.
Settlor	A natural or legal person who transfers the control of his funds to a Trustee under a document.
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
Source of funds	Means the origin of customer's funds which relate to a transaction or service and includes how such funds are connected to a customer's source of wealth.
Source of wealth	Means how the customer's global wealth or net worth is or was acquired or accumulated
Supervisory Authority	Federal and local authorities which are entrusted by legislation to supervise financial institutions, designated non-financial businesses and professions and non-profit organizations or the competent authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations
Suspicious Transactions	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any mis demeanor or felony or related to the financing of terrorism or of illegal organizations, whether committed or attempted.
Targeted Financial Sanctions (TFS)	The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings, The term Targeted Financial Sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups or organization who are sanctioned.
The Executive Office	The Executive Office of the Committee for Goods and Materials Subject to Import and Export control.

Transaction	All disposal or use of Funds or proceeds including for example deposits, withdrawals, conversion, sales, purchases, Inward remittance, outward remittance.
Trust	A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.
Trustee	natural or legal person who has the rights and powers conferred to him by the Settlor or the Trust, under which he administers, uses, and acts with the funds of the Settlor in accordance with the conditions imposed on him by either the Settlor or the Trust.
Ultimate Beneficial Owner	A person (natural) who owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a juridical person. A Natural Person who owns 25% or above of the juridical person is treated as an UBO.
UN Consolidated List	A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.
Undercover Operation	The process of search and investigation conducted by one of the judicial impoundment officer by impersonating or playing a disguised or false role to obtain evidence or information related to the Crime.
Wire Transfer	Financial transaction conducted by a financial institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.
Without Delay	Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

15. ANNEXURE–III FATF LISTED HIGH-RISK/MONITORED JURISDICTIONS Jurisdiction

S. No.	Country	High Risk Jurisdictions/ Monitored Jurisdiction
1.	Bulgaria	Jurisdiction under increased monitoring
2.	Burkina Faso	Jurisdiction under increased monitoring
3.	Cameroon	Jurisdiction under increased monitoring
4.	Croatia	Jurisdiction under increased monitoring
5.	Democratic Republic of the Congo	Jurisdiction under increased monitoring
6.	Haiti	Jurisdiction under increased monitoring
7.	Kenya	Jurisdiction under increased monitoring
8.	Mali	Jurisdiction under increased monitoring
9.	Monaco	Jurisdiction under increased monitoring
10.	Myanmar (Blacklist)	High-Risk Jurisdiction subject to Call for Action
11.	Mozambique	Jurisdiction under increased monitoring
12.	Namibia	Jurisdiction under increased monitoring
13.	Nigeria	Jurisdiction under increased monitoring
14.	Philippines	Jurisdiction under increased monitoring
15.	Senegal	Jurisdiction under increased monitoring
16.	South Africa	Jurisdiction under increased monitoring
17.	South Sudan	Jurisdiction under increased monitoring
18.	Syria	Jurisdiction under increased monitoring
19.	Tanzania	Jurisdiction under increased monitoring
20.	Venezuela	Jurisdiction under increased monitoring
21.	Vietnam	Jurisdiction under increased monitoring
22.	Yemen	Jurisdiction under increased monitoring
23.	Democratic People's Republic of Korea (Blacklist)	High-Risk Jurisdiction subject to Call for Action
24.	Iran (Blacklist)	High-Risk Jurisdiction subject to Call for Action

FATF Listed high-risk countries as of **on 28 June 2024.**
This list is to be updated as and when there is change in the list of high-risk and increased monitoring jurisdictions. Please use below link to update: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increasemonitoring-october-2022.html and https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2022.html

16. ANNEXURE – IV HIGH-RISK FACTORS

a) Customer Risk Factors

- The business relationship is conducted in unusual circumstances.
- Non-resident customers.
- Legal persons or arrangements that are personal asset-management vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Businesses or activities that are cash-intensive or particularly susceptible to money laundering or terrorism financing.
- The ownership structure of the Company appears unusual or excessively complex given the nature of the Company's business.
- Business relationships and transactions conducted other than "face to face".
- Business relationships conducted in or with countries as identified in (b) below.
- Politically exposed persons ("PEP").
- High net worth customers, or customers whose source of income or assets is unclear.

b) Country or Geographic Risk Factors

(Please refer to Annexure V- FATF Listed High Risk/Monitored Jurisdictions)

- Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries identified by the Committee as high risk.
- Countries subject to sanctions, embargos or similar measures issued by the United Nations.
- Countries classified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

c) Product, Service, Transaction, or Delivery Channel Risk Factors

- Cash and other bearer or negotiable instruments.
- Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
- Payment received from unknown or un-associated third parties