MASSIF TRADING LLC

Office No 409, Al Hind Building 7, Al Ras,
Gold Souq, P.O. Box 380261, Deira,
United Arab Emirates

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY AND PROCEDURE

MASSIF TRADING LLC

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY AND PROCEDURE

I. Revision History

Prepared by :	Legal and Compliance Officer		
Approved by:	Managing Partner		
Effective Date	01 June 2022		
Version Number	03	**Revision Date**	1 March 2024

Revision History

Version	Date	Highlight
Original	01 June 2022	ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY AND PROCEDURE
Version 2/ Revision 1	01 October 2023	REVISED AS PART OF THE ONGOING UPDATE OF POLICIES AND PROCEDURES TO MEET THE UAE'S LEGAL AND MANDATORY REGULATORY REQUIREMENTS AND DIRECTIVES ON AML/CFT.
Version 3/ Revision 2	01 March 2024	UPDATED AS PART OF THE ONGOING REVIEW OF POLICIES AND PROCEDURES TO ALIGN WITH THE LEGAL AND MANDATORY REGULATORY REQUIREMENTS AND DIRECTIVES REGARDING ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) IN THE UAE.

MASSIF TRADING LLC

II. Introduction

MASSIF TRADING LLC (hereinafter referred to as "the Company") operates as a non-manufactured precious metals trading company under the auspices of a license issued by the Department of Economic Development. As part of its operations, the Company is obligated by law to establish and maintain a formal and robust Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) compliance and sanction program.

In light of the growing global concern regarding money laundering and terrorism financing, MASSIF TRADING reaffirms its commitment to compliance with the laws and regulations set forth by the UAE government, as well as international entities such as the Financial Action Task Force (FATF), the United Nations (UN), the European Union (EU), the Organization of American States (OAS) – Office of Foreign Assets Control (OFAC), and the Central Bank of the UAE.

To uphold these standards, MASSIF TRADING has implemented stringent policies and procedures to ensure that the precious metals within its supply chain originate from legitimate sources and are not associated with criminal activities, including child labor, human rights abuses, and armed conflicts. Furthermore, the Company takes proactive measures to prevent the exploitation of precious metals for the purposes of financing terrorism or engaging in money laundering activities.

III. Policy Statement

The Company is fully dedicated to adhering to all applicable anti-money laundering, countering of financing terrorism and proliferation financing laws in its business activities. The Company is committed to only do business with customers and suppliers who are engaged in legitimate economic activity and whose money are obtained legally; will not engage in business relations with companies or individuals that are suspected to be a terrorist or a criminal organization or listed in any of the sanctions list, nor with customers from prohibited jurisdictions; and shall report suspicious transactions to the regulatory body and support and cooperate in any investigation conducted by the authorities in relation to the reported transaction. To that aim, the Company will adhere to all UAE laws and regulations, inclusive but not limited to the following:

(a) Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
(b) Cabinet Decision No. 10 of 2019 regarding Implementing Regulations of Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML-CFT Decision").
(c) 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.
(d) Cabinet Decision No. 24 of 2022 amending some provisions of Cabinet Decision No. 10 of 2019.

(e) Cabinet Decision No. 58 of 2020 regarding Beneficial Owner Procedures.
(f) Cabinet Decision No 109 of 2023 regarding Beneficial Owner Procedures.
(g) MOE Circular No. 2/2021 – Guidelines for Designated Non-financial Business and Professions.
(h) MOE Circulars concerning Update on High-Risk Jurisdictions, jurisdictions under increased monitoring and identification of countermeasures to be applied by DNFBPs
(i) MOE Circular No. 8/AML/2021 – goAML Reporting Requirements

(j) Supplemental Guidance for Dealers in Precious Metals and Stones.
(k) FATF Recommendations.
(l) 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.
(m) Cabinet Decision No. 16 of 2021 regarding the unified list of violations and administrative fines for the said violations of measures to combat money laundering and terrorism financing that are subject to the supervision of the Ministry of Justice and the Ministry of Economy.
(n) Federal Law 13 of 2007, concerning commodities subject to Import and Export Control and its amendments and applicable administrative regulations and cabinet decisions.

IV. Who is covered by this Policy

This Policy is intended to assist the Board of Directors, management, employees, customers, suppliers, and other third parties operating on the Company's behalf in understanding where AML/ CFT Laws may be violated and to assist them in making proper decisions in accordance with our corporate perspective as expressed in this Policy.

V. Prohibited Transactions

In adherence to the guidelines under AML-CFT Law 20 of 2018 Article 16.1 and AML-CFT Decision 10 of 2019 Articles 13.1, 14, 35.4 & 38, the Company shall not:

(a) Form and continue any consumer or business relationship, conduct any financial or commercial transactions, keeping any accounts under anonymous, fictitious name, pseudonym or number
(b) Enter into business agreements or conduct any transactions where complete and adequate risk-based CDD measures are not fulfilled.
(c) Conduct transactions with applicants who fail to provide competent evidence of identity.
(d) Open or maintain anonymous accounts, fictitious accounts, and other accounts which do not show the name of the account holder.
(e) Conduct business with Shell companies or institutions that have no physical presence in any country, no active business and which merely exists on paper.
(f) Engage in business transaction with entities where there is reasonable ground to believe that such entity is associated with money laundering or criminal financing activity.
(g) Accept funds that are known or believed to be the proceeds of crime.
(h) Conduct transactions with companies that are issuing or dealing in bearer shares or bearer share warrant.
(i) Enter into business agreements with or continue to maintain business ties with individuals or entities that are either known or are suspected to be a terrorist or a criminal organization, whether or not listed on any of the sanction list.
(j) Develop connections and/or enter business relationships with entities/individuals from prohibited jurisdictions or industries.

VI. Know Your Customer (KYC) Guideline

Clients will only be onboarded after have successfully completed the relevant Customer Due Diligence (CDD), either through Standard Customer Due Diligence, Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) measures applicable to their situation.

To this end, the Company may require submission of the following documents/ information:

- ✓ Corporate Customer
  - Trade License Registered business name;
  - Memorandum of Association/ Article of Incorporation
  - Tax Registration
  - Certificate of Incumbency/ Shareholding Certificate;
  - Identification cards (Passport, Visa and Emirates ID) and other details of shareholders, management, authorized signatories, and ultimate beneficial owners;
  - Country of incorporation and physical address in UAE
  - Contact information;
  - Details of business activities (nature, type, volume and value of transactions);
  - Anticipated type and volume of activities;
  - Last two years audited financial statements
  - Source of funds; and
  - Proof of standing including bank reference and introductory letter
  - Company AML and Supply Chain Policies

- ✓ Individual Customers
  - Applicant's full name (as per passport);
  - Date and place of birth;
  - Nationality;
  - Physical Address (residential and business / home country and UAE);
  - Contact details;
  - Previous personal / business activities / occupation (type and volume);
  - Anticipated type and volume of company's activities;
  - Bank reference and introductory letter; and
  - Source of funds

The Company have strict KYC procedures in place, which include validating business and individual customer identities, as well as their place of residence, before doing business with any customer. This information is regularly monitored and updated where necessary, and archived when the business relationship ends. The procedure also includes profiling of the customer's transactions in terms of size, frequency, nature, and the risks the transaction pose.

Below are the key situations when SCDD, SDD or EDD should be performed:

(i) Customer Onboarding: When a potential customer applies for account opening and engage in trading transactions with the company. SCDD, SDD or EDD is conducted as part of the onboarding process to verify the customer's identity, understand the nature of their business, and assess the risk associated with the relationship.

(ii) Occasional Transaction: When carrying occasional transactions in favour of a client for amounts equal to or exceeding AED 55000.00, whether the transaction is carried out in a single of several transactions that appear to be linked.

(iii) Ongoing Monitoring: The Company shall perform ongoing monitoring to confirm the information is up-to-date and identify any irregular or suspicious transactions. The frequency of this monitoring may be adjusted according to the risk profile associated with each customer.

(iv) Trigger Events:

- Significant changes: Initiate SCDD or EDD in response to notable changes in the customer's profile, such as shifts in ownership, modifications to corporate structure, changes in beneficial ownership, or substantial adjustments in the nature or volume of transactions.
- High-Risk Scenarios: Apply EDD for customers considered high-risk, such as politically exposed persons (PEPs) or customers from high-risk jurisdictions.
- Suspicious Activity Detection: In the event activities where there are suspicions of money laundering or terrorist financing, conduct EDD to gather additional information and assess the legitimacy of the activities.
- Policy and Regulatory Changes: Conduct SCDD or EDD when there are changes in AML/CFT regulations or internal policies that necessitate a review of existing customer information.
- Periodic reviews: Conduct periodic review of customer information, at a minimum once a year, to ensure its accuracy and relevance. The frequency of these reviews should be risk-based.
- Doubtful documentation: Where there are doubts as to the veracity or adequacy of previously obtained Customer's identification data.
- Termination of the relationship: Conduct SCDD or EDD when terminating a business relationship to ensure compliance with regulations and to assess any potential residual risks.

VII. Standard Customer Due Diligence

The Standard Customer Due Diligence (SCDD) process to be performed by the Company, at a minimum, as part of "Know your customer" measures include:

- ✓ Identification and verification/authentication of the customer's identity details, address, specimen signature, ultimate beneficial owners (UBO), authorized representatives and their compliance policies;
- ✓ Screening of the customers against local and international sanctions lists;
- ✓ Determination of whether the customer and any related parties of the customer are a politically exposed person (PEP), or related/linked to a politically exposed person;
- ✓ Investigation of whether the customer and related parties of the customer are associated with high-risk countries as defined under local and international sanctions;
- ✓ Determination of whether the customer acts on behalf and/or account of other persons;
- ✓ Regularly review customer relations, inclusive of monitoring of accounts business profile and assessment of transactions for the detection of any unusual transactions; and
- ✓ Identification and verification of the source of income.
- ✓ Identification of Ultimate Beneficial Owner

In case of legal person, the Company identifies the UBO, in accordance with Cabinet Decision No. 109 of 2023 as follows:

- the natural persons who own or exercises ultimate control over a legal person; through shares of stocks or stocks or direct or indirect ownership by 25% or more of the legal person's capital, or has the right to vote in it by 25% or more, including holding that ownership through a chain of ownership or control, or through control by any other means, such as the right to appoint or dismiss the majority of their directors.
- if more than one person participates in owning or controlling a percentage of the capital in the legal person, they shall al be treated as owners and controllers of this percentage.
- If all possible means have been exhausted and no natural person with ultimate controlling ownership is or in case of a doubt that the natural person exercising control over the legal

person through other means is the Beneficial Owner then the natural person who exercises control over the legal person through other means shall be considered as the UBO.
- Where no natural person is identified, then the natural person who holds the position of a higher management official shall be deemed as the Beneficial Owner.

Exempted from UBO identification requirement shall be as follows:

- Companies wholly owned by Federal of Local government or any other companies wholly owned by such companies.
- Governmental partner

VIII. Simplified Due Diligence

Simplified Due Diligence (SDD) is used for low-risk customers or customers who pose a lower risk of money laundering or terrorist financing activities. Simplified due diligence measures must be commensurate with low-risk elements, including the following for example:

- Verifying the Client's identity and the real beneficiary owner after starting the business relationship.
- Updating Clients' data at intervals.
- Reducing the rate of continuous monitoring rate and examination operations.
- Inferring the purpose and nature of the business relationship from the type of the established transactions or business relationship, without the need to collect information or undertake specific procedures.

IX. Enhanced Due Diligence

Enhanced Due Diligence (EDD) is used for higher-risk customers or customers who pose a higher risk of money laundering or terrorist financing activities, posing a greater risk to the company, and for potentially suspicious transactions. Notwithstanding the results of the risk assessment, application of EDD and/or update of monitoring operations may be considered in accordance with the risky customer/transaction/sector assessments under AML/ CFT laws and regulations.

EDD measures shall include:

- ✓ Obtaining and verifying further information as information on the identity of the Client, the beneficial owner, his/ her profession, and the amount of funds and information available through public databases and open sources.
- ✓ Obtaining additional information about the purpose of the business relationship or the reasons for the operations expected or actually performed.
- ✓ Updating Client Due Diligence (CDD) information in a more regular manner about the Client and the beneficial owner.
- ✓ Applying reasonable measures to determine the source of funds and wealth of the Client and the beneficial owner.
- ✓ Increasing the degree and level of continuous monitoring of the business relationship in order to determine whether they look unusual or suspicious, and to select patterns of operations that need further examination and review.
- ✓ Make the first payment through an account in the Client's name at a financial institution subject to similar due diligence standards.
- ✓ Obtain senior management approval to start or continue the business relationship with the Client.

The Company shall employ EDD measures to manage and mitigate the risks associated in dealing with customers or transactions identified as High Risk. The UAE Cabinet Decision No. 24 of 2022 defines a High-Risk Customers as including those who represent a risk:

- ✓ *"..A Client who represents a risk, either in person, or through his activity, business relationship, its nature or his geographical area, such as a Client from high-risk countries, or non-resident in a country for which does not have an identity card, or of a complex structure, or who carries out complex or unclear operations with an economic or legal purpose, or carries out intensive cash transactions, operations with an unknown third party, or conduct operation without direct confrontation, or any other high-risk operations specified by Financial Institutions, Designated Non-Financial Businesses and Professions, or the Regulatory authority."*

X. IDENTIFICATION AND ASSESSMENT OF ML/FT RISKS

A. Risk-Based Approach (RBA)

The Company adopts the Risk-based approach and rigorously implements policies and procedures in screening its prospective and existing clients and suppliers, to ensure that it deals only with customers and suppliers who are engaged in legitimate economic activity and whose money are obtained legally. To this end, the Company requires all customers and suppliers to submit necessary documents and information pertaining to their legal standing, appropriate government regulatory licenses, identity of their shareholders, identity of their ultimate beneficial owners and such other documents and information as may be relevant in order to identify and assess the ML/FT risks to which they are exposed. The evaluation shall also take into account the characteristics of the institution's customers, the products, services, or transactions offered, the countries or geographical areas involved, the distribution channels used, and ML/ TF and PF vulnerabilities the transactions pose.

The Company shall identify and assess the risk profiles of its clients and the result of risk rating applied to the customers should be used in determining the efficient allocation of AML/CFT resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures.

B. ML/FT and PF Risk Methodology

MASSIF TRADING shall adopt a comprehensive strategy that involves in-depth scrutiny of customer demographics, transaction patterns, geographical spread, and the continually evolving regulatory environment, in order to gain valuable insights into potential vulnerabilities according to which risk mitigation measures shall be customized and tailored accordingly and therefore, detect and address possible vulnerabilities to money laundering and terrorist financing while strictly adhering to local regulatory mandates.

In sum, the ML/FT/PF risk assessment methodology shall be conducted in accordance with the following process:

- Identification of the inherent risks through a review of customer risks factors for the covered period.
- Identify, understand, and assess proliferation financing risks for customers, products and services, and delivery channels.
- Evaluation and categorization of the identified risks by considering their potential impact and likelihood.
- Development and implementation of risk mitigation strategy.

- Mechanism for continuous monitoring of identified risk factors and periodic assessment of risk mitigation.
- Periodic review and reassessment, especially in the event of alterations in the corporate structure, shifts in payment methods, and significant changes in transaction volumes associated with the customer.
- Documentation of risk assessments in the risk register.

C. Risk Factors

The regulation on AML/CFT specify risk factors that should be taken into consideration by DPMS when identifying and assessing ML/FT and PF risk at both the enterprise and the customer levels. The Company considers the factors such as:

Risk Factor	% Weight Assigned
Customer Risks	16.6%
Product / Service Risks	16.6%
Geographical Risks	16.6%
Transaction Risks	16.6%
Delivery Channels Risks	16.6%
ML/TF/PF Threat Risks in accordance with NRA Results and government guidelines	16.6%

Following a risk-based approach, the Company applies the following as part of its KYC process according to the risk identified:

- Simplified Due Diligence: For Low-Risk Customers only.
- Standard Customer Due Diligence: For Medium Risk Customers
- Enhanced Due Diligence: For High-Risk Customers and/or where there is a suspicion of financial crime.

D. Customer / Counterparty Risk

Risk associated with Customer/Counterparty includes Counterparty/customer type, complexity and transparency (e.g. whether the counterparty or customer is a physical person, a legal person or a legal arrangement; if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate.

E. Geographic Risk

Risk associated with geographical areas include:

- **Country of origin of the PMS** particularly in relation to whether the country is a known production or trading hub for the type of PMS; has adequate regulations and controls (for example, is a participant in the KPCS for rough diamonds); is a High-Risk Country (e.g., is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist organizations).
- **Country of origin or residence status of the counterparty or customer** (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country particularly in relation to the locations where the transaction is conducted, and the goods are delivered.

Accordingly, MASSIF TRADING shall screen customers against the FATF blacklist and grey list, and the UN and local sanctions list during the onboarding and periodically after. In any event, MASSIF TRADING strictly prohibits business transactions with entities or individuals from countries identified as High Risk subject to a call for action by FATF, and entities and individuals under the United Nations Sanctions list and the UAE local terrorist list.

F. Delivery Channel Risk

The channel by which the counterparty/customer is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy).

G. Product Risk/ New Products and Services

Risk associated with product include type, nature, and characteristics of the products and/or services, including but not limited to quantity, quality/level of purity, price/value, form (whether physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity.

H. Transactional Risk

Risk associated with product include type, size, complexity, cost, and transparency of both the transaction (including whether the physical or virtual exchange of merchandise is involved) and the means of payment or financing—particularly in relation to whether they appear to be consistent with the counterparty or customer's socio-economic profile, local market practices, and the degree of expertise required.

I. ML/TF/PF Threat Risk

Risk associated with money laundering and terrorist financing through flow of funds that may be channeled to or from local or foreign international terrorist organizations, to meet the needs of a terrorist or terrorist organizations for terrorism-related activities, and the risks associated with the financing of proliferation efforts represent a grave threat to global peace and security. To conduct the assessment, we identify the jurisdictions where there are money laundering, terrorism, and proliferation financing risks, in accordance with the findings of Financial Action Task Force (FATF) TF Risk Assessment Guidance (2019) and its updates and quantify the risks depending the level of terrorism in the region where the prospective or existing client is incorporated or situated.

Furthermore, and in compliance with the requirements of the UAE laws for Designated Non-Financial Business or Profession, MASSIF TRADING has registered with Executive Office for Control and Non-Proliferation (EOCN) Notification System, to get timely and regular updates on UNSCR and local government sanctions updates. All potential clients and connected parties shall be screened during on-boarding and before transactions, and customers and suppliers shall be screened on an on-going basis. Any and all unresolved 'potential matches' should be reported as Potential Name Match Report (PNMR), and any and all attempted transactions related to 'confirmed matches' shall be reported as Fund Freeze report (FFR), Suspicious Transaction/ Activity Repost (SAR/ STR) in the goAML System.

Accordingly, Massif Trading shall screen customers against the FATF blacklist and grey list, and the UN and local sanctions list during the onboarding and periodically after. In any event, MASSIF TRADING strictly prohibits business transactions with entities or individuals from countries identified as High Risk subject to a call for action by FATF, and entities and individuals under the United Nations Sanctions list and the UAE local terrorist list.

XI. Reporting of Suspicious Transaction

MASSIF TRADING shall institute a system for the mandatory reporting of suspicious transactions pursuant to UAE Federal Law No. 20 of 2018 on Anti-Money Laundering, Combatting the Financing of Terrorism and Financing of Illegal Organizations and Cabinet Decision No. 10 of 2019. If MASSIF TRADING has reasonable grounds to suspect that a Transaction, attempted Transaction, or funds constitute crime proceeds in whole or in part, or are related to the Crime or intended to be used in such activity, regardless of the amount, MASSIF TRADING shall adhere to the following without invoking professional or contractual secrecy (i) directly report STRs to the FIU without any delay, via the electronic system of the FIU or by any other means approved by the FIU; (ii) respond to all additional information requested by the FIU.

Where any employee or personnel, director or officer of MASSIF TRADING knows that the client has engaged in any of the predicate crimes under the UAE Federal Law, the matter must be promptly reported to the Compliance Officer within the organization who, in turn, must immediately report the details to the Managing Director and thereafter to the FIU.

If there are reasonable grounds to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the FIU unless the compliance officer/s or unit considers, and records an opinion, that such reasonable grounds do not exist.

MASSIF TRADING's directors, officers, and employees shall not warn their customers that information relating to them has been reported or is in the process of being reported to the FIU, or communicate, directly or indirectly, such information to any person other than the FIU. Any violation of this confidentiality provision shall render them liable for criminal, civil and administrative sanctions under the UAE federal law.

XII. Governance

The Company ensures that its Management and Employees are well-equipped and have appropriate knowledge and information to effectively implement this AML/CFT Policy. Our lines of defense in ensuring that our policies are held and the risks associated to money laundering, terrorist financing and proliferation financing are detected, prevented and/or mitigated include the following:

A. First Line of Defense

This includes frontline staff and operational units directly involved in customer interactions and transactions. They are responsible for implementing AML/CFT policies and procedures, conducting preliminary customer due diligence, and promptly identifying and reporting suspicious activities.

B. Second Line of Defense

This involves the appointment of compliance officer/ MLRO, who will provide oversight, guidance, and support to the first line, ensuring that AML/CFT policies and procedures are effectively implemented and followed. Additionally, the Compliance Officer/ MLRO monitors and assess the adequacy of controls and risk management practices, and performs the following:

- ✓ Detect transactions relating to crime.
- ✓ Review the AML/CFT compliance program and processes to prevent financial crimes. And ensure that the AML/CFT framework is in line with the regulatory requirements and the ML/TF risks faced by the entity.

- ✓ Review and evaluate suspicious transactions and activities and report such transactions and activities in the form of a Suspicious Transaction Report (STR) and Suspicious Activity Report (SAR) to the FIU, UAE.
- ✓ Submit various reports like Funds Freeze Report (FFR), Partial Name Match Report (PNMR), High-Risk Country Report (HRC), High-Risk Country Activity Report (HRCA), Dealers in Precious Metals and Stones Report (DPMSR), to the Financial Intelligence Unit, UAE, where the circumstances so require.
- ✓ Conduct training for the employees, and ensure their awareness of the AML rules and regulations, and train them in the best global practices to counter the risks of financial crimes.
- ✓ Develop compliance programs, reviewing company policies, and advising management on possible risks to meet regulatory obligations;
- ✓ Ensure compliance by all Company employees and staff with the provisions of AML/CFT regulations, its implementing rules and regulations and the Company's AML/CFT and KYC Compliance Manual;
- ✓ Disseminate to its Board, officers, and all employee memorandum Circulars, resolutions, instructions, and policies issued by the UAE Regulatory Agencies in all matters relating to the prevention of money laundering;
- ✓ Serve as the liaison between the Company and UAE Regulatory Agencies in matters relating to compliance with the provisions of the AML/CFT law and its implementing rules and regulations;
- ✓ Prepare and submit to UAE Regulatory Agencies written reports on the Company's compliance with the provisions of the AML/CFT law and its implementing rules and regulation, in such form as the UAE Regulatory Agencies may determine, and within such period as the UAE Regulatory Agencies may allow in accordance with the AML/CFT law, or as amended
- ✓ Manage the compliance process and the due diligence activities and stages toward the Company, its clients, and other third-party suppliers/ service providers.
- ✓ Develop strategies for risk management and organize training programs for Company employees and other staff on compliance procedures and on laws, regulations and industry practices on money laundering and financing of terrorism and financing of illegal organizations and the means to combat them.
- ✓ Perform compliance audits to determine whether established protocols are being followed and where they can be improved, and work in coordination with all managers while reporting operation, observation and inspection results to the concerned unit managers and to the Board, for corrective action.
- ✓ Report directly to the Board when necessary, taking into account the level, confidentiality and character of the matter, and conduct all monitoring and applications of statutes related to adaptation.

C. Third Line of Defense

This comprises internal audit or independent review functions, which provide objective assurance and evaluation of the effectiveness of AML/CFT controls and processes. They conduct periodic reviews, audits, and assessments to identify weaknesses, gaps, or areas for improvement in the AML/CFT framework, reporting their findings to the management and the board of directors.

XIII. Sanction Screening

The Company recognizes the threat posed by sanctioned or blacklisted entities and individuals. As such, the Company will take appropriate precautions to ensure there are measures in place to prevent such relationships and to ensure those identified are fully investigated and the appropriate action taken on a timely basis.

As part of the KYC process, the Company has introduced appropriate systems for real time screening of customer names against Sanctions List. While establishing business relationship, names including customer, beneficial owners and other relevant names are screened against all applicable sanction list, particularly the UN Sanction List issued by the UN Security Council and local regulators' list. Written policies for the escalation and clearing of potential sanction matches are in practice and the logs/records related to the clearing of potential sanction matches are available in the system for five (05) years.

The measures include the following.

- The Company will adopt measures to regularly screen customer transactions against international and national sanction listings.
- The Company will adopt measures to upload the sanction list in sales software and block transaction under such names.
- Appropriate procedures to determine whether or not a customer identified by the sweep / screening is on a sanctioned listing.
- Finally reporting of transaction of a sanctioned customer to the FIU.

XIV. Staff Training and Recruitment

Before appointment of each employee, the HR department conducts a due diligence and ask for references from previous employers or institutions. Once appointed, each employee is given basic understanding of AML rules and company policies in this regard. All employees are required and instructed to adhere to the established AML rules in this regard. Periodic and concurrent training is also available within the organization.

XV. Record Keeping

The Company shall maintain all records pertaining to the Customer Due Diligence documentation on any transaction for at least Five (05) years following the establishment of the relationship or the completion of the transaction, regardless of whether the account or business relationship is ongoing or has been terminated.

The Company shall maintain information, correspondence, and documentation for customer identification, verification and associated due diligence and enhanced due diligence for a period of at least Five (05) years from the end of the business relationship with the client or the last transaction conducted.

The Company shall maintain records concerning the internal reporting of unusual or suspicious transactions and all records of investigations of those reports, together with the decision made, should be retained for at least a period of Five (05) years after the report has been made.

The Company shall maintain records including dates of training sessions, a description of training provided and names of employees that received the training for a period of at least Five (05) years from the date on which training was provided.

The Company shall maintain records of annual reports and any other reports that highlight the level of compliance, deficiencies, and actions, including reports submitted to the Senior Management.

The record of transactions and other identification data shall be made available to the Competent Authority upon request.

Any other records to demonstrate compliance with the AML/CFT Laws, Regulations, Notices/Circulars, Standards, and the Directives must also be retained.

APPENDIX I – COVERED TRANSACTIONS

Some examples of when application of the AML/CFT measures is (or is not) required are provided below for illustration purposes:

1. A counterparty or a customer makes cash purchases of several different items at the same time, including a variety of PMS, whether loose or mounted, and requests separate invoices for each piece. No individual invoice meets the threshold of AED 55,000; however, the total purchase price exceeds this amount. These are covered transactions.

2. A counterparty or a customer wishes to purchase one or more items with a total value meeting or exceeding the AED 55,000 threshold and places a 25 percent deposit (below the threshold) in cash. A week later, he pays another 25-percent cash installment, and after another week pays the remaining balance (which is below the threshold) in cash. The transactions are all related and are therefore covered transactions.

3. Three customers enter a retail jewellery shop and together look at different set pieces. They each decide to buy diamond or gold jewellery worth AED 50,000, and all three wishes to pay in cash on separate invoices. Although they are ostensibly different customers and each purchase is below the AED 55,000 threshold, the total amount is well over the threshold and the customers are clearly associated. These are covered transactions.

4. A gold trading company buys a consignment of gold bullion worth AED 350,000 from a wholesale merchant. The buyer places a deposit of AED 50,000 in cash and says that he will arrange for the balance to be paid along with the pickup of the bullion the next day. On the following day, a van arrives from a well-known local courier company to pick up the gold, and the driver delivers to the merchant a cashier's cheque for the balance of AED 300,000. Although the cash deposit was below the threshold, cashier's cheques (like money orders, treasury bills, bearer bonds, etc.) Are negotiable bearer instruments and, as such, are considered to be cash equivalents. This is a covered transaction.

5. A retail dealer accepts a diamond and emerald ring valued at AED 95,000 from a customer as a trade-in towards partial payment for the purchase of a diamond pendant worth AED 55,000, resulting in a net cash transfer of only AED 40,000. Although the cash portion of the payment is below the threshold level of AED 55,000, the payment-in kind in the form of the traded-in ring is considered to be a cash equivalent. This is a covered transaction.

6. A dealer in gold bullion sells coins to a retail customer for a marked-up price of AED 55,100. The customer pays in cash. The coins' market value by weight on the international exchanges on the day of the sale is AED 46,746, and their book value is AED 47,223 based on the dealer's cost at the time he originally acquired the coins. This is a covered transaction. The DPMS's obligation to apply the AML & CFT measures is based on the fact that the actual price paid in cash exceeds AED 55,000, even though neither the coins' market value nor their book value meets the threshold.

7. A diamond cutting and polishing firm wishes to buy a consignment of KP-certified rough diamonds from a local wholesaler. The two parties arrive at a final negotiated price of AED 900,000, which includes the payment being made in the form of a cash deposit of AED 50,000, with the balance being covered through several negotiable third-party promissory notes from members of the Dubai diamond exchange and other internationally recognized diamond bourses (all belonging to the world federation of diamond bourses). Although the cash deposit is less than the AED 55,000 threshold, the promissory notes are bearer negotiable instruments considered to be cash equivalents. This is a covered transaction.

8. As part of his retail jewellery business, in addition to numerous rings, necklaces, bracelets and other set pieces, an established merchant normally sells only one or two loose diamonds, worth AED 2,350 to AED 2,850 each, in an average month. This pattern was fairly stable for many years. This month, however, the

merchant notices a marked increase in his sales of loose diamonds, which reach a level of 10 stones worth an average of AED 4,250 to AED 4,750 each, all of which are paid for in cash. The next month, sales of loose gemstones continue to increase, far beyond the normal pattern. Although each sale appears to involve a different customer, and they are all individually far below the AED 55,000 threshold, they are all in cash. Once the DPMS notices the sudden change in pattern and that total cash sales of loose diamonds have reached the AED 55,000 threshold, he should begin to apply the AML & CFT measures in order to assess whether these transactions may be related and thus be categorized as covered transactions.

9. An art dealer sells a sculpture, more than two-thirds of whose value is comprised of 18k gold and fine (950) platinum, for AED 95,000 in cash. Although the intrinsic value by weight of the gold and platinum content of the statue is worth more than the AED 55,000 threshold, the art dealer is not obliged to apply the AML & CFT measures required of DPMS, since the sale of PMS does not make up a regular component of his business and he is therefore not considered to be a DPMS.

10. The customer from the above example brings the sculpture he acquired to a DPMS a week later and offers to sell it for AED 50,000, based on the content of the precious metals it contains, but he insists on being paid in cash. The dealer estimates the value of the gold and platinum he can obtain from melting down the statue to be approximately AED 66,780, before his costs. Although the amount of cash demanded is below the threshold of AED 55,000, this is a covered transaction. The DPMS should apply AML & CFT measures, based on both the value of the PMS content (which exceeds the threshold) and the appearance of structuring to avoid the AED 55,000 threshold.

APPENDIX II – 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 IV- FATF Listed High Risk 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.

MASSIF TRADING LLC

APPENDIX III – FATF LISTED HIGH-RISK JURISDICTIONS

(List was amended in accordance with the Updated List of Countries issued by the Financial Action Task Force following the plenary meeting held on 23 February 2024)

S.N.	Countries	Status
1	Iran	High-Risk Jurisdiction
2	Democratic People's Republic of Korea (DPRK)	High-Risk Jurisdiction
3	Myanmar	High-Risk Jurisdiction
4	Bulgaria	Jurisdiction under increased monitoring
5	Burkina Faso	Jurisdiction under increased monitoring
6	Cameroon	Jurisdiction under increased monitoring
7	Croatia	Jurisdiction under increased monitoring
8	Democratic Republic of Congo	Jurisdiction under increased monitoring
9	Haiti	Jurisdiction under increased monitoring
10	Jamaica	Jurisdiction under increased monitoring
11	Kenya	Jurisdiction under increased monitoring
12	Mali	Jurisdiction under increased monitoring
13	Mozambique	Jurisdiction under increased monitoring
14	Namibia	Jurisdiction under increased monitoring
15	Nigeria	Jurisdiction under increased monitoring
16	Philippines	Jurisdiction under increased monitoring
17	Senegal	Jurisdiction under increased monitoring
18	South Africa	Jurisdiction under increased monitoring
19	South Sudan	Jurisdiction under increased monitoring
20	Syria	Jurisdiction under increased monitoring
21	Turkey	Jurisdiction under increased monitoring
22	Tanzania	Jurisdiction under increased monitoring
23	Yemen	Jurisdiction under increased monitoring
24	Vietnam	Jurisdiction under increased monitoring

APPENDIX V – RED FLAG INDICATORS- PROLIFERATION FINANCING

The following list of red-flag indicators of proliferation financing is therefore by no means exhaustive.

Employees should be aware that the existence of any of the indicators listed below does not automatically imply that a transaction entails proliferation financing. Nonetheless, it signals the need for heightened due diligence or additional inquiry, enabling the MLRO to make an informed decision regarding the transaction's suspicious status.

- **Transaction involves sale, shipment, or export of dual use goods incompatible with the technical level of the country to which it is being shipped.**
- **Trade finance transaction(s) involving shipment route through country with weak export control laws or weak enforcement of export control laws.**
- **The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination. Possible TBML**
- **Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.**
- **Customer or transaction is suspected of being linked (directly or indirectly) to IRAN's nuclear weapons program.**
- **Customer or transaction is suspected of being linked (directly or indirectly) to DPRK's nuclear-related, WMD-related, or ballistic missiles weapons program.**
- **Based on the documentation obtained in the transaction, the declared value of the shipment is obviously under-valued vis-à-vis the shipping cost. (Possible TBML)**
- **A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.**
- **A shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet. Possible TBML**
- **A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.**