Al Rafidain Jewellery Trading LLC

ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM, COUNTER PROLIFERATION FINANCING, AND TARGETED FINANCIAL SANCTIONS (AML/CFT/CPF &TFS) POLICY, PROCEDURES AND CONTROLS

Summary Version V2.0- March 2026

Table of Contents

1. DOCUMENT INFORMATION

Document Title	Anti-Money Laundering, Combating Financing of Terrorism, Countering Proliferation Financing, and Targeted Financial Sanctions (AML/CFT /CPF & TFS) Policies, Procedures, and Controls.
Department	Compliance
Effective From	March 2026
Note	This document is a summary of the Al Rafidain Jewellery Trading LLC AML/CFT /CPF & TFS Policies, Procedures, and Controls.

2. DOCUMENT APPROVAL STATUS

The AML/CFT/CPF & TFS Policy Prepared by	**Name**: Vinod Singh Shekhawat **Designation:** Compliance Officer	Sign:
The AML/CFT /CPF & TFS Policy Reviewed and Approved by	**Name:** Hayder Abdulridha Hasan Alobaidi **Designation:** Owner & Manager	Sign:

Company Stamp

3. ABOUT AL RAFIDAIN JEWELLERY TRADING LLC

Al Rafidain Jewellery Trading LLC herein after referred to as the "Company", as a Designated Non-Financial Business or Profession (DNFBP), places significant importance on adhering to the UAE's Anti-Money Laundering (AML) Compliance requirements as prescribed by the Ministry of Economy. These requirements serve as an important framework for preventing and detecting money laundering activities within the DPMS industry.

To meet these obligations, the Company has implemented a comprehensive system and robust procedures aimed at safeguarding the business from potential involvement in illicit financial transactions. The company recognizes the importance of maintaining a transparent and compliant environment that fosters trust among its clients and stakeholders while contributing to the overall integrity of the UAE's financial and commercial sectors.

The Company's AML compliance measures include rigorous due diligence processes for customer onboarding and ongoing monitoring of client transactions. Prior to establishing a business relationship, the Company conducts thorough customer due diligence, verifying the identity and background of customers and assessing the nature of their transactions. This process helps identify and mitigate any potential risks associated with money laundering or terrorist financing.

The Company maintains a vigilant approach to ongoing monitoring. By regularly reviewing and analyzing client transactions, the Company ensures prompt detection of any suspicious activities or unusual patterns that may indicate potential money laundering. This proactive monitoring enables the Company to take necessary actions, such as reporting suspicious transactions to the relevant authorities, in accordance with the prescribed regulations.

The Company also maintains a strong working relationship with regulatory authorities and cooperates fully during inspections and audits. By actively engaging with relevant authorities, the Company demonstrates its commitment to upholding the highest standards of AML compliance.

4. ABOUT DPMS

Dealer in PMS (Precious Metal Stones) can be defined as an individual, legal entity, or their employee or representative, who regularly engages in the production and/or trade of precious metals or precious stones. This includes dealing with raw, cut, polished, or elaborated (mounted or fashioned) forms of precious metals or precious stones. The production and/or trade activities encompass various actions involving both raw/rough and processed/finished PMS, such as:

- Extraction: This includes mining or any other method of obtaining precious metals or precious stones.
- Refining: The process of purifying or enhancing the quality of precious metals or precious stones.
- Cutting and Polishing: Shaping and refining the appearance of precious metals or precious stones.

- Fabrication: The process of creating finished products using precious metals or precious stones.
- Import or Export: Bringing precious metals or precious stones into or out of a country.
- Purchase, Sale, Re-purchase, or Re-sale: Engaging in buying, selling, or trading of precious metals or precious stones in primary, secondary, or scrap markets.
- Barter, Exchange, or Transfer of Ownership: Swapping, exchanging, or transferring ownership of precious metals or precious stones.
- Loan or Lease Arrangements: Involves activities such as sale-leaseback, consignment, or memorandum sales.
- Possession: Holding or having temporary or permanent ownership of precious metals or precious stones. This can be part of fiduciary, warehousing, collateral, or other safekeeping arrangements. It can also be under contract for specific purposes like cutting, polishing, and refining, casting, or fabrication services.
- Loan or Lease Arrangements: Involves activities such as sale-leaseback, consignment, or memorandum sales.
- Possession: Holding or having temporary or permanent ownership of precious metals or precious stones. This can be part of fiduciary, warehousing, collateral, or other safekeeping arrangements. It can also be under contract for specific purposes like cutting, polishing, and refining, casting, or fabrication services.

5. DPMS AML/CFT OBLIGATION

- Cabinet Decision No. (134) of 2025 Concerning the Implementing Regulation of Decree-law No. (10) of 2025 on Combating Money Laundering Crimes, Combating the Financing of Terrorism and Financing the Proliferation of Arms (the “AML-CFT Decision”) identifies dealers in precious metals and precious stones (DPMS) as Designated Non-Financial Business and 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.

6. COMPLIANCE WITH LAWS

- Decree-law No. (10) of 2025 on Combating Money Laundering Crimes, Combating the Financing of Terrorism and Financing the Proliferation of Arms
- Decree-law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.
- Cabinet Resolution No. 134 of 2025 concerning the Executive Regulations of Federal Decree-Law No. 10 of 2025

- ❖ 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 Financing of Illegal Organizations.
- ❖ Cabinet Decision No. (58) of 2020 Regulating the Beneficiary Owner Procedure.
- ❖ Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions.
- ❖ Supplemental Guidance for Dealers in Precious Metals & Stones (DPMS) Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organization's Guidelines for Designated Non-Financial Businesses and Professions.

7. OVERVIEW OF MONEY LAUNDERING

Money laundering (ML) is the process by which criminals attempt to hide or disguise the true origin and Ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. If carried out success fully, money laundering enables criminal stones cape prosecution, maintain control over the proceeds of crime and continue their criminal activities.

8. STAGES OF MONEY LAUNDERING

The process of ML, regardless of its degree of complexity, is an accomplished in three stages, namely placement stage, layering stage and integration stage.

- ❖ **Placement** – Placing the criminal funds into financial system.
- ❖ **Layering** – The process of separating criminal proceeds from their source by using complex layers of financial transactions designed to hide the audit trail.
- ❖ **Integration** – If the layering process succeeds, integration schemes place the Laundered proceeds back into the legitimate economy in such a way that they appear to be normal business funds.

9. OVERVIEW OF PREDICATE OFFENCES

The AML/CFT Law defines a "predicate offence" as any act constituting an offence or misdemeanor under the applicable laws of the UAE whether this act is committed inside or outside of the UAE.

A predicate offence is therefore any crime, whether felony or misdemeanor, which is punishable in the UAE, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

10. OVERVIEW OF TERRORISM FINANCING

An offense within the meaning of the UN International Convention for the Suppression of the Financing of Terrorism (1999), where a person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

- an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex of the above-mentioned treaty, or
- any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing an act.

11. OVERVIEW OF FINANCING OF ILLEGAL ORGANISATIONS

The AML/CFT Law (AML/CFT Law Articles 3.2, 4, 29.3, AML/CFT Decision Article 1) designates the financing of illegal organizations as a criminal offence that is not subject to the statute of limitations. The Law defines the financing of illegal organizations as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by an illegal organization or by any person belonging to an illegal organization or intended to finance such illegal organization or any person belonging to it, even if without the intention to conceal or disguise their illicit origin.
- Providing, collecting, preparing, obtaining proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an Illegal organization or of any of its members, with knowledge of its true identity or purpose.

When assessing their risk exposure to the financing of illegal organizations, the Company pays special attention to the regulatory disclosure, accounting, financial reporting and audit requirements of organizations with which they conduct Business Relationships or transactions. This is particularly important where non-profit, community/social, or religious/cultural organizations are involved, especially 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.

12. PROLIFERATION AND PROLIFERATION

Proliferation Financing (PF), including Financing of Arms Proliferation, is a standalone principal offence and predicate offence to money laundering under Federal Decree-Law No. 10 of 2025, encompassing the raising, moving, or provision of funds/assets for weapons of mass destruction (WMD), their means of delivery, or related dual-use goods/technologies.

Al Rafidain Jewellery Trading LLC integrate PF risks into all controls, including Customer Risk Assessment (CRA), Enterprise-Wide Risk Assessment (EWRA), Customer Due Diligence (CDD)/Enhanced Due Diligence (EDD), transaction monitoring, red flag indicators, and STR/SAR filing.

PF Risk Indicators for DPMS:

- Customers/counterparties linked to dual-use goods, high-risk PF jurisdictions (e.g., FATF grey/black lists), unusual trade routes, or WMD-related sectors (nuclear/chemical/biological).
- Transactions involving commodities subject to non-proliferation controls under Federal Decree-Law No. 43 of 2021 or UNSCRs 1718/2231.
- Complex ownership structures, front companies, or procurement patterns inconsistent with legitimate PMS trade.

13. OVERVIEW OF TARGETED FINANCIAL SANCTIONS

The term Targeted sanctions means that such sanctions are imposed against specific individuals, groups, or undertakings. TFS refers to asset freezing and other financial prohibitions, agreed upon by the UNSC, to prevent funds, or other assets from being made available, directly, or indirectly, for the benefit of listed individuals, groups, and entities.

14. NEW TECHNOLOGIES AND VIRTUAL ASSETS (VA)

The Company is aware that Federal Decree-Law No. 10 of 2025 and its Executive Regulations explicitly cover Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs).

The Company has determined that dealing in Virtual Assets (VAs), including but not limited to cryptocurrencies, stablecoins, or Non-Fungible Tokens (NFTs), presents a high inherent risk for Money Laundering and Proliferation Financing, given the nature of its business as a Dealer in Precious Metals and Stones (DPMS).

As a mandatory, definitive internal control, the Company strictly prohibits the acceptance of any form of Virtual Asset as payment for goods or services.

Any attempt by a customer to transact using a Virtual Asset must be:

1. Rejected: immediately by the employee.
2. Documented: as a high-risk red flag in the customer's file.
3. Escalated: immediately to the Compliance Officer/MLRO.
4. Considered: for the filing of a Suspicious Transaction Report (STR) based on the attempted use of an illicit or prohibited payment method.

15. STAGES OF THE SUPPLY CHAIN AND ROLES OF DPMS

The trade in PMS consists of a complex ecosystem or supply chain from extraction of the raw mineral to eventual sale to the final customer, in which numerous participants are involved. DPMS may perform a wide variety of roles or functions relating to the trade in PMS, and in order to understand these roles and the potential ML/FT risks they entail, it is necessary to have a basic understanding of the stages of the supply chain. It should be understood that the supply chains for different PMS may have certain characteristics which are unique to that particular PMS or category of PMS. Furthermore, the supply chain is not necessarily a strictly vertical one, in that different participants may trade with each other in multiple directions at different stages of the chain, and certain stages may run concurrently or be skipped altogether. However, for the sake of convenience, these stages, and some of the major ML/FT risks to which each stage is vulnerable, may be simplified as follows:

Extraction/production: This stage may also include the sorting and grading of raw minerals, and their preparation for sale. Key ML/FT risks at this stage include but are not limited to the infiltration of the extraction/production process by criminal or terrorist organizations; vulnerability of the supply chain to the introduction of illicit PMS, or “commingling”; over-, under-, or false-invoicing and accounting fraud. This stage is also vulnerable to numerous predicate offences, such as theft, embezzlement, smuggling, and bribery/corruption.

Trading in Raw minerals: This stage of the supply chain may also involve the export and import of raw ores or rough gemstones. Moreover, the market for different types of raw PMS may have different characteristics and regulatory regimes.

Beneficiation: In this stage of the PMS supply chain, raw minerals are transferred to technically specialized intermediaries for purification and preparation for sale by various processes, such as refining/smelting in regard to precious metal ores, and cutting and polishing with respect to precious stones. This stage can also include the recycling of existing PMS (e.g., the re-smelting of scrap precious metals, or the re-cutting and polishing of precious stones). DPMS may participate in this stage of the supply chain as technical specialists (refiners, cutters, polishers, etc.), or as wholesalers, agents, buyers or sellers trading with, or on behalf of, such specialists.

Wholesale trade: In this stage, processed PMS (either refined precious metals or cut and polished precious stones), as well as finished goods (i.e.jewellery) are traded on a wholesale basis for a variety of purposes, and through diverse channels, some of which may entail the physical exchange of goods and others of which may be virtual in nature (for example, through certificates or various derivative products).Key ML/FT risks at this stage include but are not limited to commingling, trade-based ML, and other known typologies and methods associated with placement, layering and integration.

Retail trade: In this stage, beneficiated PMS or finished goods (in particular jewellery fabricated from PMS) are sold to, or acquired from, retail customers in the primary or secondary markets. DPMS involved in this stage are usually retail merchants involved in selling or buying direct to/from the public. This stage is particularly vulnerable to ML/FT risks connected with commingling, as well as to the classic ML/FT risks associated with placement, layering and integration, and to predicate offences such as fraud, theft and robbery or embezzlement, among others.

There are many different stages and transactions and counterparties involved in the precious stones and precious metals businesses. As set forth above, miners range from international companies to individuals. Intermediaries may be well established local buyers from miners, or itinerant foreign buyers, or hawalas. Retail jewelers may buy articles of used jewellery, as may direct buyers and pawnshops. Each of these businesses may present a money laundering risk. Dealers may buy from or sell to other counterparties who also work in their precious metals or precious stones businesses, or sell to the public through retail sales (which may often be anonymous). Dealers will need to consider the risks associated with each stage at which they participate. A risk-based approach should account for higher risk customers and counterparties at every stage.

In some sectors within precious metals and precious stones businesses, trust based on personal contact is an essential element of conducting business, and such trust and personal contact assist in lowering counterparty risk. In addition, each industry has trade resources, such as trade associations and directories, with which to establish some background and credit information and these should be consulted. Checks must be made upon any new counterparty that is unknown to a dealer, and particularly if also unknown within the dealer's industry. A counterparty, who proposes a transaction in diamonds, jewels or precious metals should have the knowledge, experience and capacity, financial and technical, to engage in that transaction.

16. ML/FT TYPOLOGIES

The methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organizations are continually evolving and becoming more sophisticated. Moreover, the variety of transaction and activity types involving DPMS can be very wide. It is therefore impossible to provide an exhaustive list of ML/FT typologies for DPMS, as new typologies and techniques are constantly being developed and attempted.

Nevertheless, research on the subject and analysis of case studies from around the world has identified some common methods used by criminals for the purposes of ML/FT involving DPMS. These methods broadly align with the classical stages of the ML/FT process i.e. placement, layering, and integration; however, they can also involve PMS as a vehicle for committing a predicate offence, or as the direct proceeds of crime.

The following have been identified as being amongst the common typologies used for exploiting DPMS for the purpose of ML/FT, according to the Financial Action Task Force (FATF):

- Use of PMS as an alternative to currency.
- PMS as stored value instruments/means to realize the proceeds of crime
- Laundering illegal PMS and/or the use of PMS to launder the proceeds of crime.
- Trade-based ML.
- Physical smuggling of PMS.

Controls: The compliance department will conduct the typology assessment report to identify the key risk factors and monitoring rules tunings.

17. RISK BASED APPROACH

The Company implemented the risk assessment procedures based on the NRA – National Risk Assessment guidance and the Part II—Identification and Assessment of ML/FT Risks and Part III—Mitigation of ML/FT Risks from the Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations Guidelines for Designated Non-Financial Businesses and Professions March 2021.

The company conducts ML/TF risk management in accordance with the following procedure:

- Identifying inherent risks
- Assessing of the Inherent Risks
- Design an action Plan
- Implement the action Plan
- Assessing residual risks

Our AML/CFT program is “risk-based.” That means that the AML/CFT policies, procedures, and internal controls are designed to address the risk of money laundering specific to our Company. The Risk-Based Approach (RBA) is a methodology to identify, assess, and understand the ML/TF risks to which we are exposed and implement required AML/CFT measures effectively and efficiently, to mitigate and manage the risks.

Key elements of an RBA can be summarized as follows:

- Risk Identification and Assessment - identifying ML/TF risks facing our company, given the type of customers we serve, the services we offer, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies.

- Risk Management and Mitigation - identifying and applying measures to mitigate and manage ML/TF risks effectively and efficiently.

- Ongoing Monitoring - putting in place policies, procedures, and information systems to monitor changes to ML/TF risks

- Documentation - documenting risk assessments, strategies, policies, and procedures to monitor, manage and mitigate ML/TF risks

The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios. However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

18. ML/TF RISK ASSESSMENT

Risk Assessment will be done on three levels.

A. **Entity-Wide Risk Assessment** - The Compliance Officer is responsible for ensuring, that an ML/FT risk assessment at the Entity-Level, is completed and regularly reviewed. The Compliance officer will assess the money laundering and terrorist financing risks presented by aggregate Client Risk, Supply Chain Risks, Geographic Risk, Product Risk, Channel Risk and Environmental Risks.

B. **Customer Risk Assessment** -The ML/TF risk posed by each client, Natural Person or Legal person will be assessed based on Client demographics, Jurisdictional risks, Product Risks and Channel Risks.

C. **Supplier Risk Assessment** - The ML/TF posed by Suppliers will be assessed on the Stage of Supply Chain, Jurisdictional risk, Product risks and Channel Risks.
AS per the AML/CFT requirements Designated Non-Financial Businesses & Professions (DNFPBs) are required to:

- Identify, assess, monitor, manage and take effective action to mitigate ML/TF risks using a risk-based approach that requires enhanced measures when risks are higher.
- Carry out Customer Due Diligence (CDD) with respect to the customer, beneficial ownership, and business relationship either themselves and/or with reliance on third parties that fulfil specific criteria.
- Take additional measures and precautions for politically exposed persons (PEPs).
- Maintain records on CDD information and transactions.
- Identify, assess, manage, and mitigate ML/ TF risks that arise when developing new products, business practices or delivery channels or when using or developing new technologies.
- Implement policies, procedures, and internal controls against ML/TF risks.
- Apply enhanced due diligence (EDD) when dealing with customers or entities from high risk and sanctioned countries.
- Report suspicious activities & transactions to the financial intelligence unit (FIU). DNFBPs should be protected by law from criminal and civil liability for the breach of any confidentiality clause made in this regard. Note that lawyers, notaries, other independent professionals & accountants are not required to report suspicious activities if the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.
- Not tip off clients when an STR is filed with the FIU. Tipping off should be prohibited by law.
- Have access to and share information on beneficial ownership and control of legal persons & arrangements.
- Provide records and information to competent authorities to aid in ML/TF investigations carried out by them, or as a consequence of mutual legal assistance (MLA) requests.

19. APPOINTMENT OF COMPLIANCE OFFICER

The Company appointed a dedicated compliance officer, manages the AML/CFT Compliance function. The Compliance Officer (CO) is responsible for implementation and oversight of company's compliance with AML/CFT rules and regulations, staff training, etc.

The Company ensures that the Compliance Officer Shall:

- Be an Independent staff in the organization;
- Report directly to the owner, MOE and other competent authorities;
- Be provided with sufficient resources including time, systems, tools and support staff depending on the nature, size and complexity of its business;
- Be provided with unrestricted access to all information related to products or services, business partners, suppliers, correspondent agents, customers and transactions;

20. ROLES AND RESPONSIBILITIES OF COMPLIANCE OFFICER

- The Compliance Officer is in charge of reviewing, scrutinizing and reporting STRs.
- The Compliance Officer should ensure the quality, strength and effectiveness of the Organization's AML/CFT program.
- Establishing and maintaining AML/CFT policies and procedures.
- Ensuring that the organization complies with the applicable AML/CFT laws.
- Ensuring day-to-day compliance with own internal AML/CFT policies and procedures.
- Responding promptly to any reasonable request for information if made by the Competent Authorities.
- Acting as the main point of contact in respect of handling internal suspicious transactions reports from the employees and analyze them before reporting to FIU. He / She shall also be the main contact point for coordinating with FIU and other concerned bodies regarding AML/CFT.
- Submit the threshold (AED 55,000/-) Exceeded transactions on timely manner in to the GoAML System.
- Submit Suspicious Transaction Reports to the FIU in a timely manner.
- The Compliance Officer is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organizations, for reporting suspicions to the FIU.
- Cooperate with and provide the FIU with all information it requires for fulfilling their obligations.

- The Compliance Officer is in charge of informing and reporting to senior management on the level of compliance and report on that to the relevant Supervisory Authority.
- Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters (whether internal or external) and developing AML/CFT Training calendar for ensuring all staffs are adequately trained.
- Conduct regular gap analysis on new notices/regulations/best practices issued by regulatory bodies.
- Ensure all key documents pertaining to KYC of customers, customer transactions and STR are retained for the minimum period of 5 years.
- The Compliance Officer is responsible to file the STR/SAR in GoAML FIU portal and coordinate with regulators for further investigation process.
- Working with senior management and other internal and external stakeholders to ensure that the Company's staffs are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

21. ROLES AND RESPONSIBILITIES OF THE OWNER

- The Company's owner is ultimately responsible for the quality, strength, and effectiveness of the AML/CFT framework, as well as for the robustness of its compliance culture. In this regard, the Company's owner set the so-called "tone at the top," by demonstrating their commitment to ensuring an effective AML/CFT compliance program is in place, and by clearly articulating their expectations with regard to the responsibilities and accountability of all staff members in relation to it.
- Ensure that the company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- Approves the overall business risk assessment for the Company.
- Ensures that all employees of the organization are being trained on the AML/CFT.
- Reviews the compliance issues raised by the compliance department.

22. SENIOR MANAGEMENT ACCOUNTABILITY

Senior management, including the Owner and Manager of Al Rafidain Jewellery Trading LLC, bear ultimate responsibility for the effective implementation of this AML/CFT/CPF/TFS Policy and compliance with Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025. They are personally accountable for ensuring adequate resources, oversight, and risk mitigation, and may face individual liability, including fines or imprisonment, for failures in program oversight or breaches.

Senior management shall receive periodic AML/CFT/CPF/TFS reports at least quarterly or bi-annually, covering: Enterprise-Wide Risk Assessment (EWRA) updates, Customer Risk Assessment (CRA) trends, high-risk relationships, Suspicious Transaction Reports (STRs)/Suspicious Activity Reports (SARs), Proliferation Financing (PF) and Targeted Financial Sanctions (TFS) incidents, audit findings, and remediation actions. These reports must be documented, approved, and retained for supervisory review by the Ministry of Economy.

23. KNOW YOUR CUSTOMER – KYC

KYC is an acronym for "Know Your Customer" The foremost tool of anti-money laundering / combating terrorism of financing policies and procedures is to know your customers before executing any transaction. The main objective of Know Your Customer (KYC) is to determine identity and beneficial ownership of accounts, source of funds, the nature of customer's business and more. KYC process is mandatory and not a one-time process. It is on- going and continuous.

24. CUSTOMER DUE DILIGENCE

Money Laundering and Terrorist Financing is the process of concealing the proceeds of crime. One of the major steps in preventing ML/TF is the process establishing the true identity of the customer/supplier, to enable us to assess AML/CFT risk, associated with the customer or supplier. This process is called customer due diligence.

Crimes are always planned under covers and criminals pose a best and the most respectable persons making difficult for ordinary person to realize their true identities. Hence, The Company should be vigilant while dealing with both Walk in Customers & Regular Customers.

Customer due diligence is required whenever a customer wishes to conduct a transaction with the company. Due diligence is a continuous process and should be applied at different stages of a customer's relationship with the company. It is the responsibility of all employees to apply due diligence while dealing with a customer.

Customer Due Diligence enables an organization to assess the extent to which its customer exposes to a range of risk. By performing CDD, compliance department ensures to;

- Identify and verify counterparties/customers before establishing a business relationship, such as entering contractual commitments. This identified natural or legal person or authorized and fully identified agents should then be the only person or persons to whom payment is authorized to be made, or product delivered, unless legitimate and documented business reasons exist, and any third party is appropriately identified, and its identity verified;
- Identify beneficial owners and take reasonable measures to verify the identities, such that we are reasonably satisfied that we know who the beneficial owners are. The measures which must be taken to verify the identity of the beneficial owner will vary depending on the risk. For legal persons and arrangements this should include taking reasonable measures to understand the ownership and control structure of the counterparty/customer;
- Obtain information to understand the counterparty's/customer's circumstances and business, including the expected nature and level of proposed transactions;

- The details to be obtained have been specified in the attached Customer Registration form, both for Individuals and Legal Entities;
- For processing transactions, understand the customer's source of funds;
- For continuing overall business relationship, understand the customer's source of wealth; and
- During KYC renewing schedule, update KYC information for each client, retail and corporate.

25. ENHANCED DUE DILIGENCE (EDD)

Enhanced due diligence (EDD) is to take additional measures, besides usual customer due diligence, to know more about the customer and his / her transactions to confirm that the transactions and funds are legitimate and free from any criminal link.

Enhance due diligence is not required in all circumstances; it is applied where the customer and the product/service combination are considered to be a greater risk and also in cases where there is a doubt or suspicion with regard to the activities conducted by the customer. This higher level of due diligence is required to mitigate the increased risk.

Checklist for Legal Entities (Corporate Customers

S.No.	Documents
1	Trade License copy
2	Certificate of Incorporation copy
3	Membership Certificate
4	Tenancy Contract/Utility Bill
5	VAT Certificate
6	Memorandum of Association/Articles of Association
7	Power of Attorney
8	Ownership Structure
9	For Sponsor (Passport & Emirates ID) copy
10	For Owner/partner/shareholder (Passport, Visa and Emirates ID) copy
11	For Authorized Signatories (Passport, visa, and Emirates ID) copy
12	Source of Fund (ex. Bank statement)
13	Organization chart
14	GOAML registration Screenshot

26. SANCTIONS & PEPs SCREENING

The Company is using LiveEx Shield AML software is configured to execute a real – time name screening on every customer, beneficiary / beneficial owner / partner's /shareholders, representatives, and all parties involved in the transaction activity. Every customer on boarding and Transaction will be screened related to blacklisted or sanctioned entities. Therefore, when a generated alert is investigated, the Compliance Officer / MLRO consider the following variables in order to identify possible matches:

a) Full Name
b) Nationality
c) Date of Birth
d) Place of Birth

Sanctions screening refers to the process of screening customer details against the different lists of sanctions for PEP status and whether the customer is involved in money laundering or terrorist activities. The customer details are screened in the following list:

- ❖ UNSC: United Nations Security Council Consolidated List;
- ❖ UAE - Local Terrorist List
- ❖ OFAC: Office of Foreign Assets Control - Specially Designated Nationals List (SDN)
- ❖ OFAC: Office of Foreign Assets Control - Consolidated Sanctions List;
- ❖ EU: European Union Consolidated list;
- ❖ Dow Jones; and
- ❖ Internal Watch List.

27. TRANSACTION MONITORING

The Company is using LiveEx Shield AML software, it is a well- defined transaction monitoring program is an important component of an effective AML/CFT program. As a financial services industry the Company has come under immense regulatory pressure to improve and expand monitoring and surveillance of transactions for the purpose of preventing and detecting money laundering & financing of terrorism activities.

The primary objective of the Company is to concentrate on actual risks, customer and product classification and to reduce the number of chances of company from being misused.

28. SUSPICIOUS TRANSACTION AND SUSPICIOUS ACTIVITY REPORT (STR and SAR)

The meaning of the AML/CFT Law and its implementing AML/CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds which a company has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing—any of the following:

- ❖ The proceeds of crime (whether designated as a misdemeanor or felony, and whether committed within the State or in another country in which it is also a crime).
- ❖ Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organizations.
- ❖ Being intended to be used in an activity related to such crimes.

It should be noted that the only requirement for a transaction to be considered as suspicious is “reasonable grounds” in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators, behavioral patterns, or customer due-diligence information, and it is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved.

The Company also note that transactions need not be in progress or pending completion in order to be considered as suspicious. Even past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion must be reported in accordance with the relevant requirements.

29. SUSPICIOUS ACTIVITY INDICATORS

The Company will furnish a list of Suspicious Indicators to its employees. Existence of Suspicious Indicators does not necessarily mean criminality. It is a trigger for Enhanced Due diligence and further investigation by Compliance Officer.

30. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

When identifying suspicious transactions, The Company and their management and employees, should be aware of the facts that, in relation to ML/FT crimes, there is no minimum threshold or monetary value for reporting, and that no amount or transaction size should be considered too small for suspicion. This is of particular significance where the crimes of the financing of terrorism and of illegal organizations are concerned, since typologies related to them may often involve very small amounts of money.

Please refer the below points for the few examples of potentially suspicious transaction types:

- ❖ Transactions or series of transactions that appear to be unnecessarily complex, that making it difficult to identify the Beneficial Owner, or that do not appear to have a discernible economic rationale.
- ❖ Numbers, sizes, or types of transactions that appear to be inconsistent with the customer’s expected activity and/or previous activity.

- Transactions appear to be far larger than a customer's declared income or turnover.
- Transactions involving high-risk countries, including those involving "own funds" transfers, particularly in circumstances in which there are no clear reasons for the specific transaction routing.
- Situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide customer due diligence documentation, or provide documentation that is false, misleading, fraudulent or forged.

31. TIMING OF SUSPICIOUS TRANSACTION REPORT

The Company is obliged to STR reports to the GoAML FIU portal **"without any delay**."

32. SUSPICIOUS TRANSACTIONS REPORTING USING GOAML SYSTEM

Pursuant to MOE guidelines The Company follows the GoAML portal for STR and SAR Submissions.

The GoAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units (FIU's) and is one of UNODC's (United Nations Office on Drugs and Crime) strategic responses to financial crime, including money-laundering and terrorist financing. Financial Intelligence Units play a leading role in any anti-money laundering regime as they are generally responsible for receiving, processing and analyzing reports made by entities according to the requirements of UAE regulations.

GoAML is specifically designed to meet the data collection, management, analytical, document management, workflow, and statistical needs of any Finance Intelligence Unit.

33. TIPPING OFF

- As per Federal Law and U.A.E. AML/CFT Guidelines, all suspicious transactions must be kept fully confidential and no one should inform any customer that his/her transaction is being reported as a suspicious transaction to the competent authorities.
- Non-compliance is a criminal offence and the employee involved will be terminated, immediately. Additionally, he/she is personally subject to fines, imprisonment, or both.
- Staff and senior management of The Company are strictly prohibited from informing customers, other persons or third parties, either directly or indirectly, that their transactions are being monitored, investigated, or reported to the FIU and Executive Office as suspicious transactions. Such actions are considered "Tipping-Off" and are a criminal offence.

- The Company Compliance department ensures, through ongoing training and detailed procedures, that all employees of the company are aware of the consequences of tipping-off, which include immediate dismissal in addition to fines, imprisonment, or both. The staff is being provided adequate AML/CFT training to avoid Tipping off.

- It is a federal crime for Company or their managers, employees or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction. Any person violating this prohibition is liable to a penalty of no less than **AED 100,000** and no more than **AED 500,000** and imprisonment for a term of not less than six months.

34. RECORD KEEPING

As per the AML/CFT Law Articles 16.1(a), (f); AML/CFT Decision Articles 7.2, 24, 36, 37.3), The Company, obliged to maintain detailed records, documents, data and statistics for all transactions, all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures.

The objective for records keeping is to ensure that DPMS are able to provide the basic information to reconstruct the transaction undertaken, at the request of the relevant authorities.

The Company shall keep all records of all transactions and copies of supporting documents should be preserved and details such as Customer IDs, Trade Licenses, Invoice details, EDD Documents, Account Opening Documents, and Customer Profiles etc. should be easily retrievable.

The Company will principally retain the following records from an AML/CFT perspective for five years:

A. All CDD/EDD records from the date of closure of the relationship.
B. Records of all AML/CFT training delivered.
C. Details of actions taken in respect of internal and external suspicion reports.
D. Details of information considered by the Compliance Officer in respect of an internal report where no external report is made.
E. Screening Logs

35. EMPLOYEE RESPONSIBILITIES

- Always be vigilant – report knowledge or suspicion of Money Laundering
- Know Your Customer (KYC)
- Establish true owner of funds
- Proper completion and approval of forms
- Question legitimacy when in doubt
- Report potentially suspicious or unusual transactions and activities
- Data input
- Follow all internal circulars and instructions
- Adhere to our Anti-Money Laundering policy and procedures

- ❖ Be accountable for your actions &know your obligation – Ignorance is not an excuse
- ❖ Not to knowingly assist in the laundering of criminal funds.
- ❖ Not to alert a suspected launderer

36. TRAINING AND AWARENESS

The Company offers career building and skill enhancement measures through periodic in-house and outsourced training programs as well as offering the opportunity of participation in programs conducted by regulatory and professional bodies.

In order to maintain an effective AML/CFT program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this goal, the Compliance Officer or a third party provides annual AML/CFT training to all relevant employees.

The Company segregated the Training and Awareness based on the followings;

- ❖ Training for New Employees
- ❖ On-Going Training Sessions (For Exist Employees and Senior Management)
- ❖ Continuous Professional Development (for Compliance Department)
- ❖ In order to maintain an effective AML/CFT program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this goal, the CO or a third party provides annual AML/CFT training to all relevant employees.
- ❖ A comprehensive training must be provided to all employees including its manager in charge, functional heads and owners/partners/shareholder.
- ❖ The periodic training of all employees covers this policy, the KYC procedures, UAE and global regulations, particularly the identification and reporting of suspicious transactions.
- ❖ It is the policy of the Company to provide AML/CFT training to all relevant employees within 30 days of joining the company. Relevant employees include employees with customer contact, operational staff as well as senior management.
- ❖ Refresher Training must be provided to all employees at regular intervals to remain updated with any changes in provisions, regulations and AML/CFT law.
- ❖ Objective and content of the AML/CFT Training program will be responsibility of the CO.
- ❖ The Company ensures that the Compliance Officer and other employees of the AML/CFT Compliance Department must attend external training in AML/CFT compliance every year.

37. INDEPENDENT AUDIT

The testing of our AML/CFT program will be performed at least annually (on a calendar year basis), by an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the AML/CFT Law and its implementing regulations. Independent testing will be performed more frequently if circumstances warrant. The Compliance Officer, Manager and other responsible personnel involved to ensure all the open audit points are satisfactorily closed and updates Owner on a timely basis.

As per the guidelines the Company – Independent Audit will cover the followings;

- Internal Audit Charter, Scope and Methodology of Audit
- 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, and 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.
- Submit the report to Owner and the Compliance Officer with the suggested recommendations.

38. DISCIPLINARY ACTIONS

Disciplinary actions to Employees in case of violation / breach of the Policies and procedures. The employees of the Company will receive a disciplinary action from the Senior Management not limited to verbal warnings, warning letters, dismissal and or termination depending on the severity of the action done by the employee not adhering to the Policy and Procedures.

The Company is committed to follow strict compliance with the law and a corporate culture that values and promotes honesty and integrity in operations. The Company has taken measures to detect and prevent fraud, abuse, and other non-complaints practices. The Compliance Program's Disciplinary Policy applies to all employees including executives, functional heads and managers who are active participants.

Stage 1 – Improvement Note: Unsatisfactory Performance
Stage 2 – First Warning: Failure to Comply
Stage 3 – Dismissal

39. SENIOR MANAGEMENT APPROVAL

Senior management has approved this AML/CFT compliance program in writing as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of the AML/CFT law and the implementing regulations under it. This approval is indicated by signatures below.

40. CONCLUSION

The Company and its employees fully comprehend the significance of the Sanction Screening Process and are committed to taking immediate action on the regulatory notices, sanction updates, and Local Terrorist Lists. This proactive approach is essential to identify and address any potential threats related to money laundering and terrorism financing, ultimately safeguarding the integrity of the financial system.