GILT TRADING LLC

AML POLICY

PRIVATE & CONFIDENTIAL

TABLE OF CONTENTS

1.AT A GLANCE

In an ever-evolving global financial landscape, the United Arab Emirates (UAE) recognizes the paramount importance of maintaining the integrity of its financial system. Money laundering poses a significant threat not only to the financial sector but also to national security and economic stability. To combat this illicit activity, the UAE has established a robust and comprehensive Anti-Money Laundering (AML) framework, designed to detect, deter, and prevent money laundering and terrorist financing within its borders.

This Anti Money Laundering Policy Manual serves as a cornerstone of our commitment to upholding the highest standards of financial integrity and regulatory compliance. It outlines the essential principles, guidelines, and procedures that govern the efforts of financial institutions, businesses, and individuals in the UAE to safeguard against money laundering risks.

Our AML policy manual is rooted in both national and international regulatory frameworks, including all the related Laws and Regulations prevailing in the United Arab Emirates on anti-money laundering and combating the financing of terrorism (AML/CFT) and the recommendations of the Financial Action Task Force (FATF). These measures reflect our dedication to aligning with global best practices and maintaining a proactive stance in the fight against financial crime.

Within these pages, you will find a comprehensive overview of our AML policies and procedures, tailored to the unique financial landscape of the UAE. This manual serves as a vital resource for all stakeholders, including financial institutions, designated non-financial businesses and professions (DNFBPs), and government agencies involved in AML efforts. It provides clear, concise, and practical guidance on how to identify, assess, and mitigate money laundering risks effectively.

Our commitment to combatting money laundering extends beyond regulatory compliance; it is a commitment to safeguarding the UAE's reputation as a responsible and transparent financial hub. Through stringent due diligence, continuous monitoring, and a culture of vigilance, we aim to protect our financial system from abuse and ensure that legitimate businesses can thrive in a secure and stable environment.

This Anti Money Laundering Policy Manual is a living document, subject to periodic updates to reflect evolving risks and regulatory changes. We encourage all stakeholders to familiarize themselves with its contents and to actively participate in our collective efforts to maintain the integrity and security of the UAE's financial sector.

Together, we can build a resilient and secure financial ecosystem that upholds the highest standards of integrity, trust, and transparency. Thank you for your commitment to this vital mission.

The Management

GILT TRADING LLC

2.POLICY CUSTODIAN

The custodian of this Policy Document is the Money laundering Reporting Officer of our Entity.

Role of the Policy Custodian: The policy custodian is a crucial figure responsible for overseeing and managing AML policies within our organization, which is a designated non-financial businesses and professions (DNFBP). The custodian plays a pivotal role in ensuring compliance with AML regulations and safeguarding the institution against money laundering and terrorist financing activities.

Key Responsibilities:

1. Policy Development and Review: The custodian is responsible for the development, maintenance, and periodic review of our Organisation's AML policies. This includes staying updated with the latest AML regulations and incorporating necessary changes into the policies.
2. Policy Implementation: The custodian ensures that AML policies are effectively implemented throughout the organization. This involves training employees, establishing reporting mechanisms, and fostering a culture of AML compliance.
3. Risk Assessment: Conducting risk assessments to identify and assess the institution's exposure to money laundering and terrorist financing risks. The custodian should review policies and procedures based on the risk level.
4. Record Keeping: Maintaining comprehensive records of AML policies, procedures, training programs, and compliance efforts. These records are crucial for audits and regulatory reviews.
5. Reporting: Reporting suspicious transactions or activities to the relevant authorities, such as the Financial Intelligence Unit (FIU) of the UAE. The custodian ensures that proper procedures for reporting are in place and followed.
6. Auditing and Monitoring: Regularly monitoring and auditing the institution's AML program to detect and address any weaknesses or non-compliance issues. This helps in strengthening the AML framework continually.
7. Communication: Keeping the institution's employees informed about changes in AML regulations, policies, and procedures. Effective communication is essential to ensure that all staff members are aware of their AML-related responsibilities.
8. Coordination: Collaborating with other relevant departments, such as legal, compliance, and risk management, to align AML efforts with the broader risk management framework of the organization.
9. Training and Awareness: Conducting AML training programs for employees at all levels to ensure a high level of awareness and understanding of AML policies and procedures.

3.GOVERNANCE OF ANTI MONEY LAUNDERING POLICIES IN OUR ORGANISATION

Governance Structure:

1. Board of Directors: The highest level of governance in our Organisation, (a DNFBP) is our Board of Directors. This body is responsible for setting the overall strategic direction of the organization, including its commitment to AML compliance.
2. AML Compliance Officer: The institution has appointed an AML Compliance Officer (Money Laundering Reporting Officer) who reports directly to the board or a senior management executive. This officer oversees all AML activities, including policy development, risk assessment, and compliance efforts.

Key Governance Elements:

1. AML Policy Development: The AML Compliance Officer, in collaboration with relevant departments, is responsible for developing and maintaining comprehensive AML policies and procedures tailored to the institution's specific risks and activities.
2. Risk Assessment: Regular risk assessments are conducted to identify, assess, and mitigate money laundering and terrorist financing risks. The board reviews and approves the risk assessment findings and ensures that adequate measures are in place.
3. Board Oversight: The board of Directors provides oversight and approves AML policies and significant changes to the AML framework. The board is also responsible for ensuring that adequate resources and support are provided to the AML Compliance Officer and team.
4. Training and Awareness: The AML Compliance Officer organizes AML training programs for all employees and ensures that they are aware of their AML-related responsibilities. The board monitors the effectiveness of these training programs.
5. Reporting and Communication: The AML Compliance Officer communicates regularly with the board regarding AML developments, including reporting on suspicious transactions or activities to the relevant authorities, as required by law.
6. Auditing and Monitoring: The institution conducts regular internal audits and monitoring activities to assess AML compliance. The board reviews audit findings and ensures that corrective actions are taken when necessary.
7. Record Keeping: The institution maintains comprehensive records of AML policies, procedures, training, risk assessments, and compliance efforts. These records are essential for regulatory inspections and audits.
8. External Review: Periodic external reviews and assessments of the institution's AML program may be conducted by regulators or independent auditors. The board cooperates fully with such reviews and takes appropriate actions based on the findings.

4. MLRO JOB DESCRIPTION

PRIVATE & CONFIDENTIAL

As part of our commitment to maintaining the highest standards of AML compliance and ensuring the integrity of our organization's financial activities, we have meticulously selected an MLRO whose job description is regularly been reviewed and amended. This document outlines the critical responsibilities and duties of the MLRO role within our organization in accordance with the AML regulations and guidelines established by the United Arab Emirates' regulatory authorities.

Details of the current MLRO

Name of the MLRO	: NITHIN KOCHERUKKAN SOMAN
Designation	: Administrative Officer/MLRO

Job Responsibilities

Responsible for establishing AML Compliance Program to prevent money laundering and assist the organization in complying with the relevant provisions of the Anti-Money Laundering Law.

Responsible for carrying out the AML risk assessment, preparing AML policies, procedures and guidelines and implements the same.

Monitoring all AML related issues on a day-to-day basis, evaluates and escalates the matter to the senior management and the legal authorities.

Applying Enhanced CDD measures to manage high risks once identified through:

a. Obtaining more information and investigating this information such as information relating to the Customer and Beneficial Owner identity, or information relating to the purpose of the business relationship or reasons of the transaction.

b. Updating the CDD information of the Customer and Beneficial Owner more systematically.

c. Taking reasonable measures to identify the source of the funds of the Customer and Beneficial Owner.

d. Increasing the degree and level of ongoing business relationship monitoring and examination of transactions in order to identify whether they appear unusual or suspicious.

e. Obtaining the approval of senior management to commence the business relationship with the Customer.

f. Put in place suitable risk management systems to determine whether a Customer or the Beneficial Owner is considered a PEP.

g. Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP.

h. Take reasonable measures to establish the source of funds of Customers and Beneficial Owners identified as PEPs.

i. Review the internal rules and procedures relating to combating the Crime and their consistency with the Decretal-Law and the present Decision, assess the extent to which the institution is committed to the application of these rules and procedures, propose what is needed to update and develop these rules and procedures, prepare and submit semi-annual reports on these points to senior

management, and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions.

j. Prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organisations, and the means to combat them.

k. Collaborate with the Supervisory Authority and FIU, provide them with all requested data, and allow their authorised employees to view the necessary records and documents that will allow them to perform their duties.

Also responsible for:

a. Review, scrutinise and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.

b. In case of 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, directly reporting STRs to the FIU without any delay, via the electronic system of the FIU or by any other means approved by the FIU.

c. Respond to all additional information requested by the FIU.

5. AML POLICY
GENERAL GUIDELINES

PRIVATE & CONFIDENTIAL

In line with UAE Governments Anti Money Laundering Initiatives, our organisation is committed to comply with the provisions of various statues and laws as follows:

Customer Due Diligence (CDD)

Our Organisation undertakes CDD measures to verify the identity of the Customer and the Beneficial Owner before or during the establishment of the business relationship or opening an account, or before executing a transaction for a customer with whom there is no business relationship. And in the cases where there is a low crime risk, it is permitted to complete verification of Customer identity after establishment of the business relationship, under the following conditions:

(a) The verification will be conducted in a timely manner as of the commencement of business relationship or the implementation of the transaction.

(b) The delay is necessary in order not to obstruct the natural course of business.

(c) The implementation of appropriate and effective measures to control the risks of the Crime.

Our Organisation is committed to take measures to manage the risks related to the following circumstances through verification process., where:

1. Customers carrying out occasional transactions for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
2. Carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding AED 3,500.
3. There is a suspicion of the Crime.
4. There are doubts about the veracity or adequacy of previously obtained Customer's identification data.

Our Organisation is committed to undertake CDD measures and ongoing supervision of business relationships, including;

1. Audit transactions that are carried out throughout the period of the business relationship, to ensure that the transactions conducted are consistent with the information they have about Customer, their type of activity and the risks they pose, including - where necessary - the source of funds.
2. Ensure that the documents, data or information obtained under CDD Measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories.

Our Organisation is committed to identify the Customer’s identity, whether the Customer is permanent or walk-in, and whether the Customer is a natural or legal person or legal arrangement and verify the Customer’s identity and the identity of the Beneficial Owner. This should be done using documents, data or any other identification information from a reliable and independent source as follows:

(a) For Natural Persons:

The name, as in the identification card or travel document, nationality, address, place of birth, name and address of employer, attaching a copy of the original and valid identification card or travel document, and obtain approval from the senior management, if the Customer or the Beneficial Owner is a PEP.

(b) For Legal Persons and Legal Arrangements:

(1) The name, Legal Form and Memorandum of Association

(2) Headquarter office address or the principal place of business; if the legal person or arrangement is a foreigner, it must mention the name and address of its legal representative in the State and submit the necessary documents as a proof.

(3) Articles of Association or any similar documents, approved by the relevant authority within the State.

(4) Names of relevant persons holding senior management positions in the legal person or legal arrangement.

Our Organisation is committed to verify that any person purporting to act on behalf of the Customer is so authorised and verify the identity of that person.

Our Organisation is committed to understand the intended purpose and nature of the business relationship, and obtain, when necessary, information related to this purpose.

Our Organisation is committed to understand the nature of the Customer's business as well as the Customer's ownership and control structure.

Our Organisation is committed to take reasonable measures to identity the Beneficial Owners of legal persons and Legal Arrangements and verify it, by using information, data, or documents acquired from a reliable source, by the following:

1. For Customers that are legal persons

(a) Obtaining and verifying the identity of the natural person, who by himself or jointly with another person, has a controlling ownership interest in the legal person of 25% or more, and in case of failing or having doubt about the information acquired, the identity shall be verified by any other means.

(b) In the event of failing to identify the natural person exercising control as per paragraph (a) of this Clause, or the person(s) with the controlling ownership interest is not the Beneficial Owner, the identity shall be identified for the relevant natural person(s) holding the position of senior management officer, whether one or more persons.

2. For Customers that are Legal Arrangements

Verifying the identity of the Settlor, the Trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement, and obtaining sufficient information regarding the Beneficial Owner to enable the verification of his/her identity at the time of payment, or at the time he/she intends to exercise his/her legally acquired rights.

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

1. A company listed on a regulated stock exchange subject to disclosure requirements through any means that require adequate transparency requirements for the Beneficial Owner.

2. A subsidiary whose majority shares or stocks are held by the shareholders of a holding company.

In addition to the CDD measures required for the Customer and the Beneficial Owner, Our Organisation is committed to conduct CDD measures and ongoing monitoring of the beneficiary of life insurance policies and funds generating transactions, including life insurance products relating to investments and family Takaful insurance, as soon as the beneficiary is identified or designated as follows:

(a) For the beneficiary identified by name, the name of the person, whether a natural person a legal person or a legal arrangement, shall be obtained

(b)For a beneficiary designated by characteristics or by class– such as a family relation like parent or child, or by other means such as will or estate – it shall be required to obtain sufficient information concerning the beneficiary to ensure that we will be able to establish the identity of the beneficiary at the time of the pay-out. In all cases – Our organisation shall verify the identity of the beneficiary at the time of the payout as per the insurance policy or prior to exercising any rights related to the policy. If Our organisation identifies the beneficiary of the insurance policy to be a high-risk legal person or arrangement, then we shall conduct enhanced CDD measures to identify the Beneficial Owner of that beneficiary, legal person, or legal arrangement.

Our organisation shall apply CDD measures to Customers and the ongoing business relationship on the effective date of the Law, within such times as deemed appropriate based on relative importance and risk priority. It should also ensure the sufficiency of data acquired, in case CDD measures were applied before the effective date of the Law

Our Organisation shall be prohibited from establishing or maintaining a business relationship or executing any transaction should they be unable to undertake CDD measures towards the Customer and should consider reporting a suspicious transaction to the FIU.

Even if they suspect the commission of a Crime, CDD measures should not be applied if there is reasonable grounds to believe that undertaking such measures would tip-off the Customer and we should report a Suspicious Transaction to the FIU along with the reasons having prevented them from undertaking such measures.

Our organisation commits the following:

1. Not to deal in any way with Shell Banks, whether to open bank accounts in their names, or to accept funds or deposits from them.

2. Not to create or keep records of bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.

Politically Exposed Persons (PEPs)

Our Organisation shall be required to carry out the following:

For Foreign PEPs:

(a) Put in place suitable risk management systems to determine whether a customer or the Beneficial Owner is considered a PEP.
(b) Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP.
(c) Take reasonable measures to establish the source of funds of Customers and Beneficial Owners identified as PEPs. (d) Conduct enhanced ongoing monitoring over such relationship.

For Domestic PEPs and individuals previously entrusted with prominent functions at international organisations:

a. Take sufficient measures to identify whether the Customer or the Beneficial Owner is considered one of those persons.
b. Take the measures identified in Clauses (b), (c), and (d) under the first paragraph of this Article, when there is a high-risk business relationship accompanying such persons.

Our Organisation shall take reasonable measures to determine the beneficiary or Beneficial Owner of life insurance policies and family takaful insurance. If identified as a PEP, employees shall inform senior management before the pay-out of those policies, or prior to the exercise of any rights related to them, in addition to thoroughly examining the overall business relationship, and consider reporting to the Unit a suspicious transaction report.

Suspicious Transaction Reports (STRs)

Our Organisation shall put in place indicators that can be used to identify the suspicion on the occurrence of the Crime in order to report STRs, and shall update these indicators on an ongoing basis, as required, in accordance with the development and diversity of the methods used for committing such crimes, whilst complying with what the Supervisory Authorities or FIU may issue instructions in this regard.
A specific guideline related to STR is formulated by our organisation which indicates the red flags and the procedures related to the reporting, which needs to be adhered in assessing customers and their transactions.

Targeted Financial Sanctions Screening

Our organisation is committed to the following in line with the Implementation of Targeted Financial Sanctions (TFS) on UNSCRs 1718 (2006) and 2231 (2015)

This will cover the following:
a. Targeted Financial Sanctions Screening
b. Partial Name Match Checking
c. Fund Freezing & Reporting Procedures
The detailed scope of the procedures is explained in the guideline formulated by our Organisation, specifically for this screening.

6. CLIENT ONBOARDING & KYC DOCUMENTATION

PRIVATE & CONFIDENTIAL

Our AML policy covers safeguards to help prevent money laundering and terrorist financing. One of those safeguards being to ensure the identity of the person completing the financial transactions.

A KYC (Know Your Customer) check refers to verifying that the information provided about a person is legitimate and evaluating the risks of doing business with them. With a few exceptions, the AML KYC onboarding lifecycle involves five distinct phases that are listed and explained below:

- Customer Identification Program (CIP)
- Customer due diligence (CDD)
- Enhanced due diligence (EDD)
- Account opening
- Annual review

When a prospective customer wants to open a business transaction and engage in a relationship with us, a customer (KYC) form is to be filled in.
This is a standard application form where personal information is gathered such as:

For Individuals:
- Name
- Address
- Nationality
- Date of Birth
- Proof of address & identity

For Legal entities:
- Business or Legal Entity Name
- Trade License/ Incorporation documents
- Address
- Nationality
- Proof of address
- Identity details of the Manager

After CIP, the next phase in the AML KYC onboarding lifecycle process is the customer due diligence (CDD) phase, which involves assessing the client or customer to determine whether that person or company should be given a low, medium, or high-risk AML rating.

During CDD the customer is also screened against PEP (politically exposed person) lists UN Sanction Lists

In this phase of the know your customer process, they're being evaluated and given a "risk of doing business with" score, which can then be accessed later during a KYC check.

Based on various factors (type of business, source of income/wealth, expected cash transactions, location of resident, location of the business, and other rating criteria), the customer can be classified as a low risk, moderate risk, or high risk.

Some of the basic AML compliance categories for assessing risk include:

- Customer address and domicile
- Customer's business industry
- Name and type of customer
- Anticipated types of account activities
- Foreign or domestic account
- PEP screening
- Past financial history

EDD Process (Enhanced Due Diligence)

In cases where a client is deemed to pose a higher than acceptable risk, the case is escalated to the MLRO in a process known as enhanced due diligence (EDD). EDD is the third phase in the AML KYC process flow.
When performing EDD, we follow the below industry best practices and any new regulatory requirements.

(1) EDD on High-Risk Entities

When conducting EDD on high-risk entities according to KYC AML policy, we identify all beneficial owners of each legal entity .
Legal entity customers include the following entities:

- limited liability companies
- limited partnerships
- general partnerships
- business trusts
- any similar entities formed under the laws of UAE.

(2) EDD on High-Risk Individuals

For individuals that are rated high risk, the KYC and AML process is as below on conducting EDD.
KYC requirements to review for high-risk customers:

- The purpose of the account
- Source of their funds and wealth
- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors
- Occupation or type of business (of the customer and/or other individuals with account ownership or control)
- Financial statements
- Banking references
- Domicile (where the business is organized or incorporated)
- The proximity of the customer's residence, place of employment, or place of business to the bank or other financial institution
- Description of the customer's primary trade area and whether there will be routine international financial transactions.
- Description of the business operations, the anticipated volume of currency and total sales, and list of major customers and suppliers
- Explanations for changes in account activity

Open Account or Deny Application

Only after CDD/EDD has been approved, should an account be opened in accordance with financial regulations and requirements. Account opening is the final phase in the KYC onboarding lifecycle process flow.

If after completing the process of KYC and AML evaluation of the customer, the application poses too much of a risk, then the next process is to reject the application. Otherwise, the account is opened.

Annual Review

As mentioned, the AML review does not end after onboarding a client. Depending on the risk classification of the client, there will be an ongoing/annual review of the client's transactional activities to complete the AML KYC process flow. The periodicity of the review is as follows:

- Low Risk: Every 2-3 years
- Medium Risk: Every 1-2 years
- High Risk: Every 6 months to 1 year

7. POLITICALLY EXPOSED PERSONS (PEP) DECLARATION

PRIVATE & CONFIDENTIAL

Introduction: In accordance with the Anti Money Laundering (AML) regulations and guidelines of the United Arab Emirates (UAE), this section outlines the policies and procedures regarding the identification and monitoring of Politically Exposed Persons (PEPs). PEPs pose a higher risk for potential involvement in money laundering or corruption due to their prominent public positions.

Definition of PEP: A Politically Exposed Person (PEP) is defined as an individual who holds or has held a prominent public position, both domestically and internationally, which may make them susceptible to financial crimes. PEPs can include government officials, senior executives of state-owned enterprises, judges, military officials, and their immediate family members or close associates.

PEP Declaration Process:

1. Identification of PEPs: All employees and relevant parties engaged in customer due diligence (CDD) activities are responsible for identifying PEPs during the onboarding process or ongoing monitoring.
2. Enhanced Due Diligence (EDD): Upon identifying a PEP, enhanced due diligence measures must be applied. These measures include obtaining additional information about the PEP's source of wealth, the purpose of the business relationship, and the expected nature of transactions.
3. Senior Management Approval: Before establishing or continuing a business relationship with a PEP, senior management must approve the relationship after assessing the associated risks.
4. Ongoing Monitoring: PEP relationships must be subject to continuous monitoring for any unusual or suspicious activities.

PEP Register:

Introduction: To ensure transparency and compliance with AML regulations in the UAE, the DNFBP maintains a Politically Exposed Persons (PEP) Register. This register serves as a central repository for all information related to PEPs with whom the business has a relationship.

PEP Register Contents:

1. PEP's Full Name: Include the full name of the PEP.
2. Date of Identification: Document the date on which the individual was identified as a PEP.
3. Position and Affiliation: Specify the prominent public position held by the PEP and the relevant government or international organization.
4. Source of Wealth: Provide information on the source of the PEP's wealth and financial interests.
5. Business Relationship Details: Include the nature and purpose of the business relationship, including expected transactions and anticipated account activity.
6. Enhanced Due Diligence Documentation: Attach copies of documents collected during enhanced due diligence, such as identification documents, beneficial ownership information, and records of the senior management's approval.

7. **Ongoing Monitoring Records:** Include records of ongoing monitoring, suspicious transaction reports (if any), and any changes in the PEP's status.

Access to PEP Register:

1. Access to the PEP Register is limited to authorized personnel involved in AML compliance, including the Compliance Officer and designated staff responsible for CDD.
2. Information contained in the PEP Register should be treated with the utmost confidentiality and not disclosed to unauthorized parties.

Conclusion: The PEP Declaration and PEP Register sections of this AML Policy Manual underscore our commitment to complying with UAE AML regulations. Proper identification enhanced due diligence, senior management approval, and the maintenance of a PEP Register are critical components of our AML framework. These measures help mitigate the risks associated with Politically Exposed Persons and demonstrate our dedication to upholding the highest standards of integrity and transparency in our business operations.

8. THE RISK BASED APPROACH (RBA)

Introduction: The Risk-Based Approach (RBA) is a fundamental principle in our Anti Money Laundering (AML) framework for ensuring the effectiveness of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes. This section outlines our commitment to the RBA and provides guidelines for conducting CDD and EDD in accordance with the AML regulations and guidelines of the United Arab Emirates (UAE).

Risk-Based Approach (RBA):

Definition: The RBA is a methodology for identifying, assessing, and mitigating money laundering and terrorist financing risks based on the nature and scale of our business operations. It involves tailoring our AML measures to the level of risk presented by customers, business relationships, products, and services.

Key Principles of RBA:

1. **Risk Assessment:** We conduct regular risk assessments to identify and evaluate the money laundering and terrorist financing risks associated with our business operations. This assessment takes into account factors such as customer profiles, geographical locations, and product/service offerings.
2. **Customer Risk Profiling:** Customers are categorized based on their risk level, which is determined by factors such as their industry, location, transaction history, and the presence of Politically Exposed Persons (PEPs). This categorization guides the level of due diligence required.
3. **Proportionate Measures:** Our AML measures, including CDD and EDD, are proportionate to the identified risk. Higher-risk customers and business relationships are subject to more rigorous due diligence procedures.

Customer Due Diligence (CDD):

Definition: CDD is the process of verifying the identity of customers, understanding the nature of their business, and assessing the risk associated with the business relationship.

CDD Procedures:

1. **Identification and Verification:** We obtain and verify the identity of our customers using reliable and independent sources. This includes collecting information such as name, address, identification documents, and, when applicable, beneficial ownership information.
2. **Risk Assessment:** Based on the risk profile of the customer, we determine the level of CDD required, which can range from simplified due diligence for low-risk customers to enhanced due diligence for high-risk customers.
3. **Ongoing Monitoring:** We continuously monitor customer transactions and activities to detect any suspicious or unusual behaviour.

Enhanced Due Diligence (EDD):

Definition: EDD is applied to high-risk customers, business relationships, or transactions. It involves conducting a more thorough assessment of the customer's background, purpose, and expected nature of transactions.

EDD Procedures:

1. **Source of Funds/Wealth:** For high-risk customers, we obtain information on the source of their funds or wealth, ensuring that they are legitimate.
2. **Senior Management Approval:** Before establishing or continuing a business relationship with high-risk customers, senior management approval is required.
3. **Continuous Monitoring:** High-risk relationships are subject to ongoing and intensified monitoring for suspicious activities.

Conclusion: The Risk-Based Approach is the cornerstone of our AML framework, guiding our efforts to combat money laundering and terrorist financing. Through proper Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures, we aim to identify, assess, and mitigate the risks associated with our business relationships. By tailoring our AML measures to the risk level, we demonstrate our commitment to complying with UAE AML regulations while maintaining the integrity of our operations.

9.THE LIST OF RED FLAGS

Red Flags listed below should be immediately brought to the notice of the MLRO:

The Physical Person Customer:

- Is reluctant or refuses to provide personal information.
- Is reluctant, unable, or refuses to explain: – their business activities and corporate history;
    - the identity of the beneficial owner;
    - their source of wealth/funds;
    - why they are conducting their activities in a certain manner;
    - who they are transacting with;
    - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for a real estate transaction in the country.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction.
- Makes unusual requests (including those related to secrecy) of the real estate agency, brokerage, or its employees.
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Is the signatory to company accounts (especially multiple companies) without sufficient explanation.
- Is interested in foreign company formation, particularly in jurisdictions known to offer lowtax or secrecy incentives, without sufficient commercial explanation.
- Takes an unusual interest in assisting or helping to facilitate the business arrangements of the other party to the transaction. The Legal Person or Legal Arrangement Customer:
- Cannot demonstrate a history or provide evidence of real activity.
- Cannot be found on the internet or social business network platforms (such as LinkedIn or others).
- Is registered under a name that does not indicate the activity of the company, or that indicates activities different from those it claims to perform.
- Is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations.
- Uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised the transaction.
- Has directors or controlling shareholder(s) and/or beneficial owner(s) who are also found to be representatives of other legal persons or arrangements, indicating the possible use of professional nominees. T
- Has an unusually large number of beneficiaries and other controlling interests or has authorised numerous signatories for the transaction without sufficient explanation or business justification.

- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk.
- Is incorporated/established in a jurisdiction that does not require companies to report beneficial owners to a central registry.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense. The Physical or Legal Person/Arrangement Customer:
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts or excessively quick transactions, even when it poses an unnecessary business risk or expense.
- Requires introduction to financial institutions to help secure banking facilities.
- Makes deposits or other payments from multiple accounts or sources.
- Appears to engage multiple professionals in the same country to facilitate the same (or closely related) aspects of a transaction without a clear reason for doing so.
- Provides falsified records or counterfeit documentation.
- Is a designated persons or groups (i.e., is on a Sanctions List). The transaction:
- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Appears to be between parties with a questionable connection or generates doubts that cannot be sufficiently explained by the customer.
- Appears to be between two or more parties that are connected without an apparent business or trade rationale.
- Is a business transaction that involves family members of one or more of the parties without a legitimate business rationale.
- Involves a repeat transaction (including repetitive financial arrangements) between parties over a contracted period of time.
- Is financed by a non-financial institution third party, whether a natural or a legal person, with no logical explanation or commercial justification.
- Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments.
- Involves funds received from a legal entity which subsequently goes into liquidation or receivership or is struck off the register (either voluntarily or compulsorily).
- Is executed from a business account but appears to involve personal purchases or sales.
- Involves complicated transaction routings without sufficient explanation or trade records.
- Involves the transfer of real property from a natural to a legal person in an off-market sale.
- Involves the use of multiple large cash payments to pay down a loan or mortgage.
- Involves the early repayment of a loan or mortgage (especially when penalties or losses are involved).
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves funds that are sent to, or received from, a foreign country when there is no apparent connection between the country and the client, and/or which are sent to, or received from, a low-tax offshore jurisdiction or one that is considered to pose a high ML/FT risk.
- Involves property purchased with cash, which is then used as collateral for a loan within a short period of time.
- Involves the unexplained use of powers-of-attorney or other delegation processes (for example, the use of representative offices).
- Involves persons residing in tax havens or High-Risk Countries, when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.

- Involves persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities, or who are associated with such persons.
- Involves several transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves the contribution of real estate to the share capital of a company which has no registered address or permanent establishment in the country.
- Shows signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.
- Involves unexplained last-minute changes involving the identity of the parties (for example, it is begun in one individual's name and finally completed in another's without a logical explanation for the name change, such as the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed over to the owner, or the reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.) and/or the details of the transaction (such as the amount or property valuation) and/or the details of the financing (for example, a mortgage is arranged, but cash is used as the final payment method).
- Involves circumstances in which the parties: – Do not show particular interest in the characteristics of the property (e.g. quality of construction, location, date on which it will be handed over, etc.); – Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms; – Show a strong interest in completing the transaction quickly, without there being good cause; – Show considerable interest in transactions relating to buildings in particular areas, without caring about the price they have to pay.
- Involves parties who are foreign or non-resident for tax purposes and: – Their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying or leasing, even temporarily, etc.); – They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).
- Is performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, persons with similar last names, etc.).
- Is carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Takes place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes. The Means of Payment:
- Involves cash or negotiable instruments which do not state the true payer (for example, bank drafts, cashier’s cheques, or the endorsement of a third-party cheque), especially where the amount of such instruments is significant in relation to the total value of the transaction.
- Is divided into smaller parts with a short interval between them.
- Involves doubts as to the validity of the documents submitted with loan applications.

- Involves a loan granted, or an attempt to obtain a loan, using cash collateral, especially when this collateral is deposited abroad. Other:
- The transaction involves a private contract, where there is no intention to notarise or register the contract, or if when this intention is expressed, it does not finally take place.
- There is a cancellation of the contract, especially in disregard of a clause penalising the buyer with loss of the deposit if the sale does not go ahead, or when the cancellation is agreed in a separate document, leaving the parties in possession of the original contract.
- There are subsequent additional transactions relating to the same property or rights that follow in rapid succession (for example, purchase and immediate sale of property) and which entail a significant increase or decrease in the price compared with the original purchase price.
- The agreed value is significantly different (much higher or much lower) from the real value of the property or differs markedly from market values.
- The transaction involves property development in an area considered to be high-risk for economic, environmental, or other reasons.
- The customer requests the recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction under the specific circumstances.

10.SANCTIONS LISTS & SCREENING

PRIVATE & CONFIDENTIAL

Introduction: Compliance with international sanctions is a critical component of our Anti Money Laundering (AML) framework. This section outlines our policies and procedures for screening individuals and entities against applicable sanctions lists, ensuring that we do not engage in any prohibited transactions or business relationships.

Definition of Sanctions: Sanctions are restrictions or penalties imposed by governments, international organizations, or authorities against individuals, entities, or countries that pose a threat to international peace and security, or for other policy reasons. These restrictions may include asset freezes, travel bans, or trade embargoes.

Sanction Lists:

UN Sanctions List: This includes individuals and entities subject to sanctions imposed by the United Nations Security Council.
UAE Local Terrorist List: This refers to sanctions imposed by the UAE government or regulatory authorities against specific individuals, entities, or countries.
Other International Sanctions Lists: We also consider sanctions lists issued by other relevant international bodies, such as the United States Office of Foreign Assets Control (OFAC), the European Union (EU), and other competent authorities, wherever necessary

Screening Process:

Customer Due Diligence (CDD): As part of our CDD procedures, we are committed to screening all customers and business partners against relevant sanctions lists during the onboarding process.
Ongoing Monitoring: We conduct periodic reviews and continuous monitoring of our customer base to ensure that they do not appear on any new sanctions lists or updates to existing lists.
Transaction Screening: All transactions and payment instructions are subject to real-time screening against applicable sanctions lists. Any matches or potential matches trigger enhanced due diligence and a review by our Compliance Team.
Red Flags: Our staff is trained to identify red flags that may indicate a potential sanctions violation. These include unusual transaction patterns, inconsistent customer information, or suspicious activity.

Handling Matches:

Immediate Action: If a match or potential match is identified during screening, it is reported to the Compliance Team immediately.
Freezing of Assets: In the event of a confirmed match with a sanctions list, we freeze the assets and suspend the business relationship with the individual or entity as required by law.
Reporting: We promptly report any sanctions violations to the relevant UAE authorities, as well as any other competent authorities, as required by law.

Training and Awareness:

Staff Training: We ensure that all employees are trained in recognizing and dealing with sanctions-related issues as part of our ongoing AML training program.
Periodic Updates: Our staff is kept informed of changes in sanctions lists and updates to our screening procedures.

Conclusion: Our commitment to compliance with international sanctions is unwavering. The Sanction Lists & Screening section of this AML Policy Manual outlines our procedures for identifying and mitigating risks associated with individuals, entities, or countries subject to sanctions. By these policies we uphold the highest standards of integrity and transparency in our business operations, thereby safeguarding our organization from involvement in any unlawful activities.

11.SUSPICIOUS TRANSACTIONS REPORTING

PRIVATE & CONFIDENTIAL

In the context of Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regulations, the reporting of suspicious transactions is a critical component of a comprehensive AML program for any business operating in the United Arab Emirates (UAE). This manual section outlines the procedures and guidelines for identifying, documenting, and reporting suspicious transactions to ensure compliance with AML/CFT regulations and to protect our business from becoming unwittingly involved in illicit financial activities.

I. Definition of Suspicious Transactions:

A suspicious transaction is any transaction or activity that raises reasonable doubts about the legitimacy or legality of the funds, regardless of the amount involved. Suspicious transactions can manifest in various forms and may include, but are not limited to:

1. Unusual Transactions: Transactions that are inconsistent with a customer's known history, business, or financial profile, including unexpected large purchases or sales.
2. Complex Transactions: Transactions with no apparent economic or lawful purpose or where the transaction structure is unnecessarily complex.
3. Rapid Funds Movement: Swift movement of funds in and out of accounts, often without a clear business rationale.
4. Frequent Currency Exchange: Frequent and sizable currency exchanges with no clear explanation.
5. High-Risk Customers: Transactions involving high-risk customers as identified through customer due diligence (CDD) measures.
6. Non-Disclosure of Information: Customers who are reluctant to provide required identification, information, or documentation.
7. Structuring Transactions: Transactions designed to evade reporting requirements by splitting a large amount into smaller, less conspicuous amounts.

The red flags listed in the previous section of this manual enlists the situations in which additional enquiries should be made regarding the legitimacy of the transactions.

II. Reporting Procedure: To ensure effective suspicious transaction reporting, the following procedure should be adhered to:

1. Identification: Staff members must be trained to recognize and be alert to red flags and indicators of suspicious transactions. This includes knowing the customer's typical transaction behaviour.
2. Documentation: Any staff member who identifies a suspicious transaction or activity should promptly document the details in writing. This documentation should include the customer's information, transaction details, and the reasons for suspicion.
3. Reporting Authority: Suspicious transactions must be reported immediately to the designated Compliance Officer or AML Officer within the organization. If there is a suspicion involving the Compliance Officer, the report should be made to the next higher authority.
4. Internal Review: Upon receiving a suspicious transaction report, the Compliance Officer or designated authority must initiate an internal review to determine the validity of the suspicion.

5. Escalation to Authorities: If the suspicion is substantiated during the internal review, the Compliance Officer should submit a Suspicious Transaction Report (STR) to the UAE's financial intelligence unit (FIU) as required by local AML/CFT regulations. The STR should contain all pertinent information while maintaining customer confidentiality. MLRO raises an STR through the goAML system, which includes all relevant information about the suspected crime, including:

    - Background.
    - Parties involved.
    - Reasons for the report.
    - Possible red flags related to money laundering or financing of terrorism.

6. When required by FIU, MLRO should give additional details as required by FIU

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

8. Non-Retaliation Policy: Our organization strictly prohibits any retaliation against employees who report suspicious transactions in good faith. Confidentiality should be maintained throughout the process.

PROCEDURE TO FILE AN STR

- The transaction is brought to the Notice of MLRO (Money Laundering Reporting Officer)
- MLRO verifies suspicious transactions or activities with the underlying documents and circumstances.
- MLRO should act upon further on the instruction of FIU.
- MLRO, officials or staff, shall not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard.

12.TARGETED FINANCIAL SANCTIONS PROCEDURE

PRIVATE & CONFIDENTIAL

Our organisation is committed to the following in line with the Implementation of Targeted Financial Sanctions (TFS) on UNSCRs 1718 (2006) and 2231 (2015)

This will cover the following:

a. Targeted Financial Sanctions Screening
b. Partial Name Match Checking
c. Fund Freezing & Reporting Procedures

The detailed scope of the procedures is explained below:

1.Implement screening procedures on all parties of a transaction or provided services as per the definition of a DNFBP in Article (3) of Cabinet Decision No (10) of 2019 concerning the Implementing Regulations to ensure they are not linked with persons or entities or organizations listed under UNSCR 1718 (2006) and 2231 (2015).

Implement Enhanced Due-Diligence (EDD) procedures on all transactions, including trade transactions, linked to North Korea and Iran.

Verification of cross-border transactions suspected of being related to unauthorized trading of Dual-Use Goods

Report immediately (without delay) all confirmed or potential matches related to any individuals or entities designated pursuant to the above-mentioned UNSCRs.

Reporting shall cover:

• Any confirmed match by raising a Funds Freeze Report (FFR) via GoAML within 5 business days from implementing any freeze measures.

• Any potential match by raising a Partial Name Match Report (PNMR) via GoAML within 5 business days from implementing any suspension measures.

• Any suspicious transactions or activity that may be related to designated individuals or entities pursuant to the above-mentioned UNSCRs by raising an STR/SAR via GoAML to the UAE Financial Intelligence Unit.

Procedures on TFS reporting via the GoAML Platform:

When a 'confirmed match' to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, we are required to take the following necessary actions:

1) Implement all necessary measures without delay as outlined in the Cabinet Decision (74) of 2020, Guidance on Targeted Financial Sanctions issued by the EO-IEC.

2) Report any freezing measure, prohibition to provide funds or services, and any attempted transactions to the Ministry of Economy and the Executive Office – IEC via the GoAML platform within two business days by selecting the Fund Freeze Report (FFR); and

3) Ensure all the necessary information and documents regarding the 'confirmed match' is submitted along with the FFR.

4) Uphold freezing measures related to the 'confirmed match' until further instructions are received from Executive Office – IEC; and

5) Notify and share a copy of the report with Ministry of Economy through this email: sanctions@economy.ae

When a 'potential match' to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, we are required to take the following necessary action:

1) Suspend without delay any transaction and refrain from offering any funds or services, as outlined in the Guidance on Targeted Financial Sanctions, and Guidance for Licensed DNFBPs on the Implementation of Targeted Financial Sanctions.

2) Report the 'potential match' to the Ministry of Economy and the Executive Office – IEC via the GoAML platform by selecting the Partial Name Match Report (PNMR);)

3) Ensure all the necessary information and documents regarding the name match is submitted; and

4) Uphold suspension measures related to the 'potential match' until further instructions are received from Executive Office – IEC via the GoAML platform on whether to cancel the suspension or implement freezing measures.

5) Notify and share a copy of the report with Ministry of Economy through this email sanctions@economy.ae

You are also instructed to adhere the following procedures stipulated by the Supervisory Authorities in this regard.
Freezing Funds As per the Sanctions List & Local Lists

1. Any person shall, Without Delay and without prior notice, freeze Funds as per the Sanctions List and Local Lists without limiting such measure to funds that may only be used to perpetrate a certain act, conspiracy, threat or agreement related to terrorism and its financing or WMD proliferation and its financing. The freezing measure shall include the following:

a. Funds owned or controlled, wholly or jointly, directly, or indirectly, by the Listed Person or funds owned or controlled, wholly or jointly, directly or indirectly, by a person or organization acting on behalf or at the direction of the Listed Person;
b. Funds derived or generated from funds under sub-paragraph (a) of the present Article.

1. Any person must notify the Office of any freezing measures taken pursuant to Paragraph (1), within five business day of the date of the freezing.
2. No person shall make funds available or provide financial or other related services, whether in whole or in part, directly or indirectly, to any of the persons or entities mentioned above, except upon authorization from the Office in line with the provisions of the present Decision, and after coordination with the Council or the UN Security Council or the relevant Sanctions Committee, and in line with Cabinet decisions regarding the issuance of Local Lists, or relevant UNSCRs, as the case may be.
3. In all cases, the rights of bona fide third parties shall be taken into account when implementing any freezing measure.

13.TRAINING & AWARNESS

1.Preamble

Money laundering poses a significant risk to the integrity and reputation of our jewellery business in the United Arab Emirates (UAE). To mitigate this risk and comply with local AML regulations, it is essential to establish robust training and awareness programs. This note outlines the training and awareness initiatives within our AML policy manual to ensure that our employees and external stakeholders are well-informed and equipped to identify and prevent money laundering activities effectively.

2. Purpose of Training and Awareness

The primary objective of our training and awareness programs is to:

- Educate our employees about money laundering risks and methods.
- Foster a culture of compliance and vigilance across the organization.
- Enable employees to identify and report suspicious activities promptly.
- Ensure that our business operations comply with UAE AML laws and regulations.

3. Training Framework

3.1. AML Training for Staff

All employees, including management, are required to undergo AML training. This training includes:

- Understanding the nature and significance of money laundering.
- Recognizing the red flags and indicators of suspicious transactions.
- Familiarizing with our internal AML policies, procedures, and reporting mechanisms.
- Understanding the legal and regulatory framework governing AML in the UAE.

3.2. Training Frequency

New employees must complete AML training within their first month of employment. Afterward, all employees will undergo refresher training Quarterly. Additionally, employees in high-risk roles will receive specialized training as needed.

3.3. Training Methods

Training will be conducted through various methods, including in-person sessions, e-learning modules, workshops, and scenario-based exercises. The training content will be updated regularly to reflect changes in AML laws and emerging risks.

4. Awareness Programs

4.1. Management's Role

Our senior management is committed to promoting a culture of compliance and awareness. They will lead by example by actively participating in AML training and consistently reinforcing the importance of AML compliance to all employees.

4.2. Employee Awareness

Employees will be encouraged to remain vigilant and report any suspicious transactions or activities promptly. We will establish open communication channels to ensure that employees can raise concerns without fear of reprisal.

4.3. External Stakeholder Awareness

Our AML policy manual will also emphasize the importance of AML compliance to our external stakeholders, including suppliers, customers, and business partners. We will work towards creating awareness campaigns and partnerships to promote AML compliance across the jewellery industry in the UAE.

5. Documentation and Record-Keeping

We will maintain records of all AML training sessions, including attendance and assessment results. These records will be kept confidential and made available to relevant authorities upon request. Additionally, we will document and retain all reports of suspicious activities, investigations, and actions taken in response.

6. Conclusion

Effective training and awareness programs are essential components of our AML policy, reflecting our commitment to combating money laundering and protecting the reputation of our jewellery business in the UAE. We will regularly review and update our training and awareness initiatives to adapt to evolving AML risks and regulatory requirements.

By ensuring that all employees are well-informed and proactive in preventing money laundering, we can contribute to the broader efforts of the UAE in maintaining a robust AML framework and upholding the integrity of our industry.

14.RECORD KEEPING

INTRODUCTION

Record keeping is an essential component of an effective Anti-Money Laundering (AML) policy in any business in the United Arab Emirates (UAE). It serves as a critical tool in combating money laundering and terrorist financing activities by providing a comprehensive trail of transactions, customer information, and due diligence efforts. This elaborate note outlines the importance of record keeping, its legal requirements in the UAE, and best practices to ensure compliance with AML regulations.

2.IMPORTANCE OF RECORD KEEPING

2.1. AML Compliance: Record keeping is crucial for demonstrating compliance with AML regulations, which require businesses to maintain accurate and up-to-date records of customer transactions and due diligence efforts.

2.2. Transaction Monitoring: Detailed records enable the monitoring of transactions, allowing businesses to identify suspicious or unusual activities that may indicate potential money laundering.

2.3. Reporting Obligations: Proper records assist in fulfilling reporting obligations to the UAE's regulatory authorities, such as the Financial Intelligence Unit (FIU) and the Central Bank of the UAE, when suspicious transactions are detected.

2.4. Auditing and Investigations: In the event of regulatory audits or law enforcement investigations, comprehensive records can prove invaluable in providing evidence of compliance and assisting authorities in their inquiries.

3. LEGAL REQUIREMENTS IN UAE

3.1. Federal AML Laws: The UAE has established federal AML laws that require businesses, including jewellery stores, to maintain records of customer transactions and due diligence documentation.

3.2. Customer Due Diligence (CDD): Jewellery businesses in the UAE must conduct CDD on all customers, including collecting and retaining identification documents, transaction details, and business relationships.

3.3. Transaction Records: Records must include information on the value, date, and nature of transactions, as well as the parties involved, including the customer and any third parties.

3.4. Retention Period: Records should be retained for a minimum of five years from the date of the last transaction or the end of the business relationship with the customer, whichever is later.

3.5. Reporting: Suspicious transactions must be reported promptly to the FIU, and relevant records should be made available to authorities upon request

4. BEST PRACTICES FOR RECORD KEEPING

4.1. Data Accuracy: Ensure that all records are accurate, complete, and up-to-date. Implement robust data validation processes to minimize errors.

4.2. Secure Storage: Store records securely to prevent unauthorized access or tampering. Implement encryption and access controls for electronic records.

4.3. Regular Audits: Conduct regular internal audits to verify the accuracy and completeness of records. Address any discrepancies promptly.

4.4. Training: Train employees on record-keeping procedures and the importance of AML compliance. Ensure that they understand their responsibilities in maintaining records.

4.5. Technological Solutions: Consider investing in AML software solutions that can automate record-keeping processes and help in transaction monitoring.

4.6. Document Retention Policy: Develop a clear document retention policy that outlines the procedures for storing, archiving, and destroying records in accordance with legal requirements.

4.7. Reporting Mechanisms: Establish clear procedures for reporting suspicious transactions to the FIU and for cooperating with law enforcement agencies.

5.CONCLUSION

Incorporating comprehensive record-keeping practices into your AML policy manual is vital for ensuring compliance with AML regulations in the UAE's jewellery industry. These practices not only facilitate compliance but also contribute to the overall integrity and reputation of your business while aiding in the prevention of money laundering and terrorist financing activities. Regularly update and review your record-keeping processes to stay current with evolving AML regulations and best practices.