

Company Name: IST Real Estate LLC

Address: Office#950, Tamani Arts Offices, Business Bay, Dubai, UAE.

Policy Number: 001

**Policy Title: Anti-Money Laundering and Counter-Terrorist Financing
(AML/CTF) Policy**



Anti Money Laundering (AML) Policy

Anti-Money Laundering (AML) policies are designed to prevent financial crimes, specifically money laundering and the financing of terrorism. They involve a set of procedures, laws, and regulations that financial institutions and Designated Non-financial Business Professionals (DNFBP) entities must follow to detect and report suspicious activity. Designated Non-financial Business Professionals (DNFBP) includes Real Estate Brokers which leads us to prepare AML policy. The following laws and regulations are the founding principles of this policy document:

1. Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations, and its Implementing Regulation.
2. Cabinet Decision No (10) of 2019 concerning the Executive Regulations of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
3. Cabinet Decision No. 74/2020 Concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions.
4. Federal Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
5. Cabinet Decision No. 24 of 2022 amending some provisions of Cabinet Resolution No (10) of 2019 on the Effective Regulations of Federal Decree Law No. (20) of 2018 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations.



Table of Contents

1. INTRODUCTION AND APPLICATION.....	6
2. MONEY LAUNDERING AND TERRORISM FINANCING	7
3. OBLIGATIONS.....	7
4. DISCLOSURE REQUIREMENTS	7
5. RISK ASSESSMENT.....	8
6. CUSTOMER DUE DILIGENCE (“CDD”).....	9
6A. Simplified Customer Due Diligence (“Simplified CDD”)	10
6B. Standard Customer Due Diligence (“Standard CDD”)	10
6C. Enhanced Customer Due Diligence (“Enhanced CDD”).....	11
7. POLITICALLY EXPOSED PERSONS IDENTIFICATION PROCESS	12
8. EDD & EDD MEASURES.....	13
9. CDD MEASURES FOR DOMESTIC, FOREIGN, AND INTERNATIONAL ORGANIZATIONS	16
9A. CDD Measures for Foreign PEPs:.....	16
9B. CDD Measures for Domestic PEPs:.....	17
9C. CDD Measures for International Organization PEPs:.....	18
10. MONITORING AND REPORTING.....	19
11. COOPERATION WITH AUTHORITIES.....	20
12. CONTINUOUS MONITORING	21
13. MISCELLANEOUS	23
APPENDIX 1	24
FACTORS OF HIGHER RISK SITUATIONS	24
FACTORS OF LOWER RISK SITUATIONS	25
APPENDIX 2.....	26
ENHANCED DUE DILIGENCE OBLIGATION	26
APPENDIX 3A	27
i) TF RED FLAGS	27
ii) PF RED FLAGS	30
APPENDIX 3B – CASH TRANSACTION MEASURES & AML COMPLIANCE	36
APPENDIX – 4 KNOW YOUR CUSTOMER (KYC) FORM	39
APPENDIX – 5 AUTOMATED CUSTOMERS DUE DILLIGENCE FORM (CDD)	42



Acronyms / Terms

AML-CFT Law	<ol style="list-style-type: none"> 1. Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations, and its Implementing Regulation. 2. Cabinet Decision No (10) of 2019 concerning the Executive Regulations of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations. 3. Cabinet Decision No. 74/2020 Concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions. 4. Federal Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations. 5. Cabinet Decision No. 24 of 2022 amending some provisions of Cabinet Resolution No (10) of 2019 on the Effective Regulations of Federal Decree Law No. (20) of 2018 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations.
AML	Anti Money Laundering
CFT	Combating the Financing of Terrorism
DNFBP	Designated Non-Financial Businesses and Professions
CDD	Customer Due Diligence
ECD	Enhanced Customer Due Diligence
KYC	Know Your Customer
STR	Suspicious Transaction Reporting



UNSC	United Nations Security Council
SAR	Suspicious Activity Report
PEP	Politically Exposed Person
TF	Terrorists Financing
UBO	Ultimate Beneficial Owner
NPO	Non-Profit Organization
RBA	Risk Based Approach
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
LFI	Licensed Financial Institutions
CBUAE	United Arab Emirates Central Bank
Personnel	Personnel means the directors, officers, full-time, part-time, and seconded employees of company, and anyone working on company's behalf
REAR	Real Estate Activity Report



1. INTRODUCTION AND APPLICATION

- 1.1. This Anti-Money Laundering Policy is established, and may be amended by, the MLRO after the approval from senior management.
- 1.2. The Anti-Money Laundering Policy ("AML Policy") applies to the company. It applies to all directors, officers, full-time, part-time, and seconded employees, and anyone working on the company's behalf, e.g. consultants and representatives. Personnel are expected to act in a manner that will enhance the company's reputation for honesty, integrity, and reliability.
- 1.3. The AML Policy will not give answers for every ethical or legal situation. If Employees have any doubts about the right thing to do, they should seek advice.
- 1.4. If Employees violate the company's policies and procedures or any of the laws that govern the company's business, the company will take immediate and appropriate action up to and including termination of employment.
- 1.5. This AML Policy sets out the key principles and obligations in relation to the AML Framework to identify and assess the Money Laundering ("ML")/Terrorism Financing ("TF") risks to which the company is exposed to ("ML/TF", respectively the "AML" measures, or more broadly "AML"), as defined below.
- 1.6. For the purpose of this AML Policy, a counterparty comprises of: company's shareholders, companies that company has invested in ("Portfolio Investments"), Employees, financial institutions, service providers and any business relationship. A 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by such law, and which is expected, at the time when the contact is established, to have an element of duration.
- 1.7. The owner(s) of the company is/are ultimately responsible for compliance with all relevant laws, regulations, rules, and professional standards applicable to JAB, whereunder those with respect to AML. This is set out in more detail in the Governance Framework.
- 1.8. The owner(s) of the company is/are responsible for the day-to-day execution of the risk management function. This is set out in more detail in the Governance Framework.



2. MONEY LAUNDERING AND TERRORISM FINANCING

- 2.1. Money Laundering is the process by which it attempts to hide and disguise the true origin and ownership of the proceeds from criminal activities, thereby avoiding prosecution, conviction, and confiscation of criminal funds.
- 2.2. Terrorism Financing means: the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

3. OBLIGATIONS

- 3.1. The main obligations for the company and its Personnel under this AML Policy are as follows:
- 3.1.1. Perform a risk assessment on overall activities, including contemplated activities.
 - 3.1.2. Perform an individualized counterparty due diligence on a risk-sensitive basis; and
 - 3.1.3. report to and cooperate with the competent authorities (if required).
- 3.2. Company complies with all applicable laws and regulations wherever company conducts business, enters, or maintains business relationships.

4. DISCLOSURE REQUIREMENTS

- 4.1. No payment greater than equal to **AED 55,000** (either one single payment or in parts) should be accepted in cash (including notes, coins, or travelers' cheques in any currency). This does not mean any payment below this limit will be valid and legal and should not raise suspicion. Professional skepticism should be retained at all levels.
- 4.2. Staff who collect cash payments are asked to provide the details of any cash transaction over AED 55,000 to the MLRO so that precautionary checks can be performed and proper reporting can be performed.
- 4.3. Company, in the normal operation of its services, accepts payments from individuals and organizations. If an employee has no reason to suspect or know that money laundering activity is taking place and if the money offered is less than AED 55,000 in cash as payment



or part payment for goods/services offered by the company, then there is no need to seek guidance from the MLRO.

4.4. If a member of staff has reasonable grounds to suspect money laundering activities or proceeds of crime, or is simply suspicious, the matter should still be reported to the MLRO. If the money offered is **AED 55,000 or more** in cash then payment must not be accepted until guidance has been received from the MLRO even if this means the person has to be asked to wait.

4.5. Any officer involved in a transaction of this kind should obtain information as per criteria set in Customer Due Diligence and Enhanced due diligence if required.

5. RISK ASSESSMENT

5.1. Company has adopted the AML Policy and has put procedures in place to mitigate the risk it may become directly or indirectly involved in actual or potential money laundering activities, or in terrorist financing activities.

5.2. Company takes a risk-based approach to prevent, manage, and mitigate AML offences, including (but not limited to):

5.2.1. identification of the risk of AML to which it could be exposed.

5.2.2. categorizing such risk in accordance with its internal risk categorization methodology;

5.2.3. defining and implementing appropriate measures to mitigate the identified risk.

5.3. In the risk-based approach, Company considers the nature and the size of its activities, and the risk factors related to:

5.3.1. types of counterparties and/or (ultimate) beneficial owners (UBO);

5.3.2. types of (envisaged) products with their counterparties.

5.3.3. types of (envisaged) services with their counterparties.

5.3.4. the delivery channels.

5.3.5. type of business activities of the company; and

5.3.6. the countries and geographical locations where the company is doing business.

5.4. The company examines, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. The company increases its degree and nature of monitoring of the business relationship, to determine whether those transactions or activities appear suspicious.

<https://www.opensanctions.org/>

<https://www.uaecic.gov.ae/en-us/un-page>

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>



6. CUSTOMER DUE DILIGENCE ("CDD")

(Conducted at the time of customer onboarding and through continuous ongoing monitoring)

- 6.1. The company will, before the establishment of a business relationship or the conducting of a transaction, as part of all due diligence measures shall:
 - 6.1.1. identify and verify the identity of its counterparty and the (ultimate) beneficial owner(s);
 - 6.1.2. assess the level of AML risk such counterparty could present; and
 - 6.1.3. decide the intensity (i.e., simplified, standard or enhanced due diligence)
- 6.2. Document the entire process of due diligence & keep records for at least five years.
- 6.3. The AML compliance officer will monitor the due diligence performed by responsible Employees and shall review the assessment performed and any supporting documentation, as relevant.
- 6.4. It is prohibited that accounts are kept under fictitious names.
- 6.5. **"Customer due diligence measures" comprise, where applicable:**
 - 6.5.1. identifying the counterparty and verifying the counterparty's identity based on documents, data or information obtained from reliable and independent sources; and
 - 6.5.2. identifying the (ultimate) beneficial owner and taking reasonable measures to verify his/her identity so that the professionals are satisfied that they know who the (ultimate) beneficial owner is, including, as regards legal persons, fiduciaries, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the counterparty.
- 6.6. The following is a non-exhaustive list of risk variables that should be considered when determining to what extent it shall apply counterparty due diligence measures:
 - 6.6.1. The purpose of the customer i.e., investment for business or personal use
 - 6.6.2. Expected timer period for the investment.
 - 6.6.3. The Risk profile, and
 - 6.6.4. The results of financial sanctions/Politically Exposed Person ("PEP")/negative media screening.



6A. Simplified Customer Due Diligence (“Simplified CDD”)

6.7 In case of low AML risk, company may opt to apply a Simplified CDD. The conclusion that simplified CDD is appropriate will always be based on a risk assessment. Company can carry out a prior assessment of the cases in which simplified CDD will be used. This will be done by means of a prior risk analysis, taking into account the risk factors on the basis of which the low-risk counterparties will be identified. Factors of potentially lower AML risk situations areas are set out in Appendix 1.

6.7.1 Simplified CDD consist of a verification of the declared identity of the counterparty against the relevant public register and/or other available sources, and assessing the information received on the purpose and intended nature of the business relationship.

6B. Standard Customer Due Diligence (“Standard CDD”)

6.8 Standard CDD is carried out by the company when onboarding and entering into a business relationship and the carrying-out of a transaction its counterparties and there are no material factors of increased AML risks found. Standard CDD consists of:

- identifying the customer with whom the business relationship is entered with;
- verifying the identity declared by the customer in the application form against documents, data, or information from reliable and independent sources; and
- where applicable, identifying the (ultimate) beneficial owner(s) when different to the Customer.



6C. Enhanced Customer Due Diligence (“Enhanced CDD”)

- 6.9 Enhanced CDD will be applicable when an increased AML risk is identified. Factors of potentially increased AML risk situations are set out in this document.
- 6.9.1 Enhanced CDD will also be applicable when dealing with natural persons or legal entities established in third countries which do not or insufficiently apply AML measures.
- 6.9.2 In the event of cross-border correspondent and other similar relationships with respondent institutions in third countries and, contingent upon the assessment of a higher risk with respondent institutions in Member States, credit institutions and other institutions involved in such relationships, Comp-any shall:
- gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision.
 - assess the respondent institution's anti-money laundering and anti- terrorist financing controls; and
 - obtain prior approval from the MLRO before establishing business relationships.



7. POLITICALLY EXPOSED PERSONS IDENTIFICATION PROCESS

Purpose

The purpose of this section is to establish a comprehensive Politically Exposed Person (PEP) identification process within the Customer Due Diligence (CDD) framework to mitigate the risk of potential money laundering or corruption activities associated with politically exposed individuals.

Definitions

- Politically Exposed Person (PEP): An individual who is or has been entrusted with prominent public functions or individuals closely related to them.

- PEP Categories:
- Foreign PEPs
- Domestic PEPs
- International Organization PEPs

Risk Assessment

Prior to onboarding a customer, a thorough risk assessment will be conducted to determine if the customer falls within the category of Politically Exposed Persons. This risk assessment will take into consideration the type of business relationship, geographic location, and nature of the customer's activities.

Customer Screening

The company will employ advanced screening tools and databases to identify potential PEPs associated with the customer. This screening will be conducted at the initial onboarding stage and regularly thereafter based on the risk assessment.

Company will use in-house PEP register as well as <https://www.opensanctions.org/> (which is updated on daily basis) to search the customer for politically exposed person. Additionally, UAE local list and UN consolidated Sanctions list and social media scanning will also be used.

UAE local List: <https://www.uaecic.gov.ae/API/Upload/DownloadFile?FileID=2017e120-bb9f-4e17-ae49-f13984c70a1f> US Sanctions List

UN Sanctions List: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list> Local List



8. EDD & EDD MEASURES

For customers identified as PEPs, enhanced due diligence procedures will be applied. This includes obtaining additional information on the source of wealth, monitoring transactions more closely, and conducting periodic reviews to ensure ongoing compliance. The policy will be periodically updated and approved by the senior management.

Source of Wealth Verification

For identified Politically Exposed Persons (PEPs), the company shall conduct a comprehensive verification of the source of wealth. This includes obtaining detailed information about the PEP's financial background, business interests, and assets.

Ongoing Monitoring

EDD measures shall encompass continuous monitoring of the PEP's transactions, relationships, and activities throughout the business relationship. Any unusual or significant transactions shall be promptly investigated and documented.

Periodic Reviews

Periodic reviews of the PEP's profile shall be conducted at predefined intervals based on the assessed risk. These reviews will include an updated risk assessment, verification of current information, and reassessment of the necessity for enhanced due diligence.

Senior Management Approval

Prior to establishing or continuing a business relationship with a PEP, senior management approval is required. The approval process shall include an assessment of the risks associated with the PEP and the appropriateness of the business relationship.

Enhanced Documentation Requirements

For PEPs, the company shall require additional and updated documentation to verify their identity, including but not limited to, recent utility bills, official identification documents, and documentation supporting the declared sources of wealth.



Escalation Procedures

In the event of any significant changes in the PEP's profile or if red flags indicative of higher risk emerges during the course of the business relationship, the case shall be escalated for further investigation and appropriate action.

Reporting to Regulatory Authorities

The company shall have a protocol in place for reporting any findings during enhanced due diligence that raise suspicions of money laundering, corruption, or other illicit activities to the relevant regulatory authorities in accordance with applicable laws and regulations.

Training and Guidance

Employees responsible for conducting enhanced due diligence measures shall receive specialized training on the specific requirements and procedures related to PEPs. Regular guidance and updates will be provided to ensure the effective implementation of EDD measures.

Record Keeping

All findings related to the PEP identification process, including risk assessments, screening results, and due diligence outcomes, will be thoroughly documented and maintained in accordance with applicable laws and regulations.

Training and Awareness

Employees involved in the customer onboarding process will receive regular training on identifying and handling politically exposed persons. Awareness programs will be conducted to ensure an initiative-taking approach to PEP identification.

Compliance Officer / MLRO is responsible for training a new team member on AML regulations. Start by explaining what AML laws are? and why they matter legally? and implications on the Company in case of non-compliance? Ask every employee to go through our company's AML policy in detail so they grasp the main rules and duties along with explanation of KYC, CDD & EDD forms. Lastly, they will sign a form saying they have read



and agree to follow the policy, making sure everyone knows how important it is to stick to these standards.

Reporting

Any identified PEPs or suspicious activities will be promptly reported to the appropriate regulatory authorities in compliance with applicable laws and regulations.

Regular Review

The Politically Exposed Person identification process will be subject to regular review and updates to ensure its effectiveness in mitigating potential risks. Any changes in regulations or industry best practices will be promptly incorporated into the process.



9. CDD MEASURES FOR DOMESTIC, FOREIGN, AND INTERNATIONAL ORGANIZATIONS

When it comes to Foreign and Domestic Politically Exposed Persons (PEPs), specific CDD measures are applied to mitigate the potential risks associated with individuals who hold or have held prominent public positions. Here are definitions for CDD measures in the context of Foreign and Domestic PEPs:

9A. CDD Measures for Foreign PEPs:

1. Enhanced Identification and Verification:

- Rigorous identification and verification procedures should be applied to ascertain the identity of foreign PEPs, including the collection of official identification documents, proof of address, and other relevant information.

2. In-Depth Background Checks:

- Conduct thorough background checks on foreign PEPs to understand their political affiliations, public roles, and potential exposure to corruption or bribery.

3. Source of Wealth Verification:

- Obtain detailed information about the foreign PEP's source of wealth to ensure that it is legitimate and not derived from illicit activities.

4. Continuous Monitoring:

- Implement continuous monitoring of transactions and relationships involving foreign PEPs to detect any unusual or suspicious activities.

5. Ongoing Risk Assessment:

- Regularly reassess the risk associated with the business relationship with a foreign PEP, taking into consideration any changes in their political status or activities.



9B. CDD Measures for Domestic PEPs:

1. Enhanced Identification and Verification:

The company will apply stringent identification & verification procedures for domestic PEPs, including the collection of official identification documents and additional information.

2. Political Affiliation Checks:

Verify the domestic PEP's political affiliations and roles through publicly available information and relevant databases.

3. Transaction Monitoring:

Implement transaction monitoring systems to scrutinize the financial activities of domestic PEPs and detect any unusual patterns or high-risk transactions.

4. Ongoing Risk Assessment:

Conduct periodic risk assessments for domestic PEPs to account for any changes in their political roles, exposure, or potential risks associated with their activities.

5. Escalation Procedures:

Establish clear escalation procedures to oversee any red flags or suspicious activities identified during the business relationship with a domestic PEP.



9C. CDD Measures for International Organization PEPs:

1. Identification and Verification:

Develop mechanisms to identify customers associated with international organizations and verify their identities.

2. Risk Assessment:

Assess the risk level associated with customers connected to international organizations.

Consider the type of organization, the role of the individual within the organization, and any relevant contextual factors.

3. Enhanced Due Diligence (EDD):

Implement enhanced due diligence measures specific to international organization PEPs, such as obtaining additional information on their functions and roles.

4. Documentation Requirements:

Request and maintain documentation that reflects the customer's relationship with the international organization, as well as any relevant information about their source of wealth.

5. Senior Management Approval:

Obtain approval from senior management before establishing or continuing a business relationship with an individual connected to an international organization.

6. Training and Awareness:

Provide specialized training to staff involved in customer due diligence to enhance their ability to identify and manage risks associated with international organization PEPs.



10. MONITORING AND REPORTING

- As part of the ongoing relationship with the counterparty, ongoing AML monitoring will be conducted on a risk-based approach and where needed or otherwise required. In case unusual transactions, such as data changes, payments or withdraws, or activities potentially linked to money laundering, are identified, further investigation will take place. Transactions / activities not consistent with the initially declared purpose or nature of the relationship may also be further investigated.
- If any member of staff knows or suspects that money laundering is taking place, they must report it to the MLRO as soon as the knowledge or suspicion first strikes them. Any delay leaves them open to the two charges of failure to report, and of assisting an offence. There is no need for them to ascertain the nature of the crime which leads them to suspect that the unusual transaction may be an instance of money laundering. However, they must be able to explain what made them suspicious.
- An internal log will be maintained by the MLRO with information on all unusual transactions escalated to the MLRO, the investigations conducted for each report received and the outcome of such investigation, including whether the instance was reported to the authorities or not.
- The MLRO will report to the owners, on an as needed basis, on unusual or suspicious transactions, their status and the outcome of investigations conducted.
- The MLRO will also file the following:
 - A STR or SAR as required to the authorities where payment against the sale or purchase of free hold land is done by following way (whether for a portion or the entire property):
 - Physical cash equal or exceeding AED 55,000 (single payment or through several transactions)
 - Virtual assets where the account is in the sanctions list
 - Transaction was converted from or to a virtual asset for a portion or the entire property value where the transaction is suspicious.



11. COOPERATION WITH AUTHORITIES

All Employees are obliged to cooperate fully with the FIU or any other Governmental authorities responsible for combating AML, if required. If needed, this could include reporting suspicious transactions and cooperating with the authorities, or inform promptly, on their own initiative, the appropriate authority when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence, or terrorist financing is being committed or has been committed or attempted, in particular in consideration of the person concerned, its development, the origin of the funds, the purpose, nature and procedure of the operation.

The identity of the Employees or authorized representatives having provided such information is kept confidential by the authorities, unless disclosure is essential to ensure the regularity of legal proceedings or to establish proof of the facts forming the basis of these proceedings.



12. CONTINUOUS MONITORING

Compliance Officer is required to ensure that the documents, data or information obtained under KYC, CDD & EDD (if applicable) are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories. Ongoing monitoring allows the Company to ensure that the purchase & sale of real estate is being used in accordance with the customer or relationship profile developed through KYC during onboarding, and that transactions are normal, reasonable, and legitimate.

For the repeating customer and if the business relationships prolong six months then it is required to that the customer profile must be reviewed and updated either after six month or at least upon the expiry of the ID, the trade license or the ID of any person authorized to make transactions on behalf of the customer, whichever comes first. At this time, the MLRO must conduct ongoing monitoring on the customer which must consist of the following:

The copy of ID must be held in the records during the review of a customer profile.

CDD (and, where appropriate, EDD) must be repeated and the customer profile updated, including the information required under AML regulations.

CDD and EDD must also be repeated whenever there is a change in the profile of the customer;

MRLO must scrutinize the transactions concluded by a customer to ensure that transactions are consistent with its knowledge of the customer, the customer's business, risk profile, the source of funds and where necessary, source of the customer's wealth; and

MLRO must review transaction monitoring results for the customer to determine whether any STR/SARs or other reports have been filed or whether the customer's behavior has generated alerts.

Unless otherwise required, such as in the cases above mentioned, MLRO should update the KYC information on customers and counterparties on a risk-based schedule, with KYC on higher-risk customers being updated more frequently. KYC updates should include a refresh of all elements of initial KYC.

Furthermore, MLRO should conduct EDD when the revised risk rating demands it or if the customer/counterparty's history of transactions is not consistent with its profile and the expectations established at account opening. In particular, if the customer/counterparty's transactions/behavior



have resulted in the filing of an STR/SAR with the FIU, the MLRO should review the customer/counterparty profile and the activity that led to the report and make a determination as to whether the risk rating should be raised or the relationship should be terminated. MLRO may consider requiring that the customer/counterparty update them as to any changes in its beneficial ownership. Even if this requirement is in place, however, MLRO must not rely on the customer/counterparty to notify it of a change, but must still update KYC on a schedule appropriate to the customer's risk rating.



13. MISCELLANEOUS

Occasional non-compliance:

Subject to applicable law and regulation, the MLRO may occasionally and in specific events decide at its sole discretion that this AML Policy can be deviated from. However, proper reasoning along with documentation will be maintained by MLRO and MLRO will ensure that no law is being breached and that the transaction is as per guidelines of AML authorities within UAE.

Interpretation:

In case of uncertainty or difference of opinion on how a provision of this AML Policy should be interpreted, the opinion of the MLRO shall be decisive.

Governing law and jurisdiction:

This AML Policy is governed by the laws of the United Arab Emirates.

Complementarity to law and Articles of Association:

This AML Policy is complementary to the provisions governing the MLRO as contained in laws and regulations and the Articles of Association. Where this AML Policy is inconsistent with laws and regulations, the latter shall prevail. Where this Code is consistent with the Articles of Association but inconsistent with laws and regulations, the latter shall prevail.

Partial invalidity:

If one or more provisions of this AML Policy are or become invalid, this shall not affect the validity of the remaining provisions. The MLRO after the approval from Partners may replace the invalid provisions by provisions which are valid and the effect of which, given the contents and purpose of this Code is, to the greatest extent possible, similar to that of the invalid provisions.



APPENDIX 1

FACTORS OF HIGHER RISK SITUATIONS

Customer Risk Factors

- a) the business relationship is conducted in unusual circumstances.
- b) customers that are resident in geographical areas of higher risk.
- c) companies that have nominee shareholders or shares in bearer form.
- d) businesses that are cash-intensive; and
- e) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

Product, service, transaction, or delivery channel risk factors

- a) products or transactions that might favor anonymity.
- b) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures.
- c) payment received from unknown or unassociated third parties; and
- d) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Geographical risk factors

- a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems.
- b) countries identified by credible sources as having significant levels of corruption or other criminal activity.
- c) countries subject to sanctions, embargos or similar measures issued by, for example, the UAE Government or the United Nations; and
- d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.



FACTORS OF LOWER RISK SITUATIONS

Customer risk factors

- a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- b) public administrations or enterprises from countries or territories having a low level of corruption; and
- c) counterparties that are resident in geographical areas of lower risk.

Product, service, transaction, or delivery channel risk factors

- a) products, service, transactions, or delivery channel where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (particularly, certain types of electronic money).

Geographical risk factors

- a) the customer is in one of the Member States of the UAE
- b) the customer is in a third country having effective anti-money laundering and counter terrorist financing systems.
- c) the customer is in third countries identified by credible sources as having a low level of corruption or other criminal activity; and
- d) the customer is in third countries which, based on credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent.



APPENDIX 2

ENHANCED DUE DILIGENCE OBLIGATION

Below are the customers/clients type where company will conduct Enhanced Due Diligence:

- (a) A foreign PEP, or his family members and close associates.
- (b) A high risk domestic PEP, or his family members and close associates.
- (c) A high risk international organization PEP, or his family members and close associates.
- (d) Individual belonging to country included in Black List.
- (e) Instruction to perform a transaction (which may include cash) anonymously
- (f) The client transferred any funds without the provision of underlying services or transactions
- (g) Unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)
- (g) Unaccounted payments received from unknown or un-associated third parties
- (h) Where client gives instruction to make any transaction on behalf of shell companies with nominee shareholder(s) and/or director(s)
- (i) Set-up or purchase companies or business entities that have no obvious commercial purpose
- (j) Multi-layer, multi-country, and complex group structures.



APPENDIX 3A

1. RED FLAGS

The consolidated list of TF and PF red flags can be found below.

i) TF RED FLAGS

The following red flags are specific to terrorist financing cases related to the UAE and other regional countries:

- Conducting of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries, particularly in higher-risk locations.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- An individual or entity's online presence supports violent extremism or radicalization.
- Irregularities during the CDD process which could include, but is not limited to:
 - Inaccurate information about the source of funds and/or the relationship with the counterparty.
 - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the ultimate beneficiary of the funds or goods.



- Suspicion of forged identity documents.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g., crowdfunding initiative, charity, non-profit organization, nongovernment organization, etc.).
- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The customer receives/ sends money declaring it for personal needs, but the actual purposes are for trade related transactions. The intention of the customer is to hide the underlying nature of the transaction and circumvent the regulatory requirements thereon. Further, the customer could potentially be trying to hide the details of the ultimate beneficial owner (UBO) of the corporation to circumvent the possible sanctions screening detection.
- Sudden spurt in currency exchange transactions by a group of resident / non-resident customers who could be from similar geographic locations, profession, or age group, who are acting as mules to assist larger cash smuggling groups.

The list below covers other red flags that may be applicable to the broader TF context:

- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted when the inclusion of such information would be expected.
- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and Financial Action Task Force (FATF) as non-cooperative countries and territories).



- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations, which are subject to weaker ML/TF controls.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted, or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Client conducted travel-related purchases (e.g., purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.



ii) PF RED FLAGS

The following red flags are specific to proliferation financing cases related to the UAE and other regional countries:

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
- Dealings with dual-use (DUG) or controlled goods. For example:
 - Chemicals
 - DUG (wire nickel, inverters, etc.)
 - Dealings with sanctioned goods or under embargo. For example:
 - Weapons Oil or other commodities
 - Luxury goods (for DPRK sanctions)
- Identifying documents (e.g., bill of lading, sales purchase agreement, etc.) that seem to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Description of goods on trade or financial documentation is nonspecific, innocuous, or misleading.
- A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
 - o For companies, they are importing high-end technology devices which is not in accordance with their trade license.



o For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide humanitarian aid.

- Transactions involved in sale, shipment, or export of DUG (Dual Use Goods) is incompatible with technical level of the country being shipped (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).

- Complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.

- Complex legal entities or arrangements that seem to be aiming to hide the UBO.

The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern, e.g., DPRK, Myanmar and Iran.

- The use of representative offices of UNSC sanctioned banks to remit DPRK labours money to DPRK.

- The use of extensive currency exchange networks to transfer bulk cash to Iranian nuclear program.

- The use of cyber-attacks by the DPRK regime to steal funds from FIs and crypto currency exchanges.

- A trade finance transaction involves a shipment route (if available) through a country with weak export control laws or weak enforcement of export control laws.

- When the flows of funds exceed those of normal business (revenues or turnover).

- The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination.

- Based on the documentation obtained in the transaction, the declared value of the shipment is obviously undervalued vis-à-vis the shipping cost.



- A shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flag hopping, or using a small or old fleet.
- The account holder conducts financial transactions in a circuitous manner.
- The customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.
- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the originators appear to be entities who may relate to a state sponsored proliferation program (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.
- A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding.
- The transaction involves receipt of cash (or other payments) from third party entities.
- that have no apparent connection with the transaction.
- Customer activity does not match the customer's business profile, or end-user information does not match the end-user's business profile.
- Inconsistencies are identified across contracts, invoices, or other trade documents, e.g., contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.



- Customer approaches to receive high value transactions which are initiated from high-risk jurisdictions/ bordering to high-risk jurisdictions claiming that the origin of funds are from sale of property or any other assets in the homeland. However, the actual source is not supported with adequate supporting documents and often a fake transaction.

The list below covers other red flags that may be applicable to the broader PF context:

Customer Profile Risk Indicators

- o During onboarding, a customer provides vague or incomplete information about their proposed trading activities. The customer is reluctant to provide additional information about their activities when queried.
- o During subsequent stages of due diligence, a customer, particularly a trade entity, or its owners or senior managers, appears in sanctioned lists or negative news, e.g., relating to past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes.
- o The customer is a person connected with a country of proliferation or diversion concern, e.g., through business or trade relations, as identified through the national risk assessment process or by relevant national CPF authorities.
- o The customer is a person dealing with DUG, goods subject to export control, or complex equipment for which he/she lacks technical background, or that is incongruent with their stated line of activity.
- o A customer affiliated with a university or research institution is involved in the trading of DUG or goods subject to export control.
- o A new customer requests a letter of credit transaction while awaiting approval of a new account.



Account and Transaction Activity Risk Indicators

- A transaction involves a person or entity in a foreign country of proliferation concern.
- A transaction involves a person or entity in a foreign country of diversion concern.
- A transaction involves financial institutions with known deficiencies in AML/CFT controls and / or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Wire transfer activity shows unusual patterns or has no business or apparent lawful purpose.
- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g., companies do not have a high level of capitalization or display other shell company indicators. Countries or the private sector may identify more indicators during the risk assessment process, such as prolonged periods of account dormancy followed by a surge of activity.
- Business or compliance personnel identify links between representatives of companies exchanging goods, e.g., the same owners or management, physical address, IP address, or telephone number, or activities that appear to be coordinated.
- A transaction or account activity involves an originator or beneficiary that is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services).
- The customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals.



- o Transactions are made on the basis of “ledger” arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies that maintain a record of transactions made on each other’s behalf. Occasionally, these companies will make transfers to balance these accounts.
- o Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes.
- o Use of cash or precious metals (e.g., gold) in transactions for industrial items.
- o Buyer entity & seller entity are owned by the same / related UBOs and using the trade channels to launder money.
- o Sudden increase in online sales by particular vendors (online auction / ecommerce sites).
- o Unrelated individuals are sending remittances from foreign countries to low-income resident individuals from some unrelated nationalities, who are acting as mules to receive money for unknown beneficiaries.



APPENDIX 3B – CASH TRANSACTION MEASURES & AML COMPLIANCE

1. Policy Statement

The entity acknowledges the money laundering risks associated with cash-intensive transactions in the real estate sector and is committed to complying with:

- **Federal Decree-Law No. (20) of 2018** on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).
- **Cabinet Decision No. (10) of 2019**, which mandates reporting of large cash transactions.

2. Due Diligence Measures for Cash Transactions

A. Acceptable Cash Transactions

- The entity **only accepts cash payments up to AED 55,000 per transaction.**
- Any cash payments **above AED 55,000 must be reported via REAR** to the UAE Financial Intelligence Unit (FIU).

B. Customer Due Diligence (CDD) Requirements

For all cash transactions, the entity must:

- **Verify buyer and seller identities** (Emirates ID/passport, visa details).
- Obtain **proof of residential address** (utility bill, tenancy contract).
- Determine the **source of funds** (bank statements, salary slips, asset sale receipts).

C. Enhanced Due Diligence (EDD) Requirements

EDD is mandatory if:

1. The customer is a Politically Exposed Person (PEP).
2. The customer is from a FATF blacklisted/high-risk country.
3. The source of funds is unclear or unverifiable.
4. The transaction is funded using cryptocurrency.
5. The customer is attempting to break down large transactions into smaller ones (structuring).
6. The buyer and seller have no apparent relationship or business connection.

EDD Steps:

- ✓ Conduct sanctions screening against UN, EU, and UAE watchlists.
- ✓ Require bank statements for the past six months to verify income sources.
- ✓ Obtain additional supporting documents (employment letter, tax filings, business ownership proof).



✓ In case of cryptocurrency-funded transactions, ensure:

- Funds were converted into fiat currency through a regulated exchange.
- Wallet ownership verification through blockchain analysis tools.
- No involvement in crypto mixing or privacy coins.

3. Transaction Monitoring & Internal Red Flags

The entity will monitor all transactions for suspicious indicators, such as:

Frequent high-value cash transactions from the same customer.

Multiple small transactions structured to avoid REAR reporting threshold.

Use of third-party payments (cash received from someone other than the buyer).

Transactions involving customers from high-risk jurisdictions.

Cryptocurrency-funded transactions without clear documentation.

Customers reluctant to provide source of funds verification.

If a red flag is detected, the entity must immediately file a Suspicious Transaction Report (STR) via goAML.

4. Reporting & Record-Keeping

A. REAR Reporting Requirements (Real Estate Activity Report)

• Who must report?

- o Real estate brokers, agents, and developers accepting cash transactions exceeding AED 55,000.

• What must be reported?

- o Buyer & seller details (name, nationality, ID details).
- o Property details (type, location, transaction value).
- o Cash amount received.
- o Due diligence measures applied.
- o Source of funds verification.

• Where to report?

- o Through the goAML portal of the UAE Financial Intelligence Unit (FIU).
- When to report?



o Immediately after accepting the cash payment.

B. Record-Keeping Requirements

- All cash transactions and supporting documentation must be retained for a minimum of five years.
- Records must be readily available for regulatory audits and FIU inspections.

5. Sample REAR Report Format

Date	Transaction ID	Buyer Name	Seller Name	Property Details	Cash Amount (AED)	EDD Applied	Source of Funds Verified?	Crypto Used? (Y/N)	Suspicious ? (Y/N)	Reported to FIU (Y/N)
05/03/2025	REAR-2025-001	Ali Al Rashid	ABC Properties	Apartment 405, Downtown Dubai	150,000	Yes – PEP Screening	Yes	No	No	Yes
12/03/2025	REAR-2025-002	John Smith	XYZ Real Estate	Villa 9, Palm Jumeirah	250,000	Yes – High-Risk Country	No	No	Yes	Yes
15/03/2025	REAR-2025-003	Wei Zhang	Dubai Realty LLC	Office 12, Business Bay	300,000	Yes – Crypto Wallet Screening	Yes	Yes	Yes	Yes



APPENDIX – 4 KNOW YOUR CUSTOMER (KYC) FORM

Know Your Customer (KYC) Form

The customer is required to provide the following information for establishing Business relationship with the Company:

Full Name as per Identity Document:	ID / Passport or a similar identification number:
<input type="text"/>	<input type="text"/>
Father's Name:	Mother's Name:
<input type="text"/>	<input type="text"/>
Residential address, telephone # and e-mail:	Date & Place of birth:
<input type="text"/>	<input type="text"/>
Gender (Male, Female, Others):	Employer Name:
<input type="text"/>	<input type="text"/>
Representation on behalf of Self / Third Party / Company. Please specify:	
<input type="text"/>	
Permanent address, telephone numbers, ZIP Code and e-mail:	
<input type="text"/>	
In case the customer is a Free Zone entity, please specify:	

Residential Status in UAE:

Business name, address, telephone numbers and e-mail; (In case of Businesses only):

Customer type:

- ☐ Single ☐ Joint ☐ Sole Proprietor ☐ Minor
☐ Other (To be specified)

Registration number of Business:

Date of registration/incorporation of business; (In case of Businesses only):

Nationality or place of birth:

Place of registration/incorporation of business:

Nature of business, locations involved and type of counter parties:

Ownership and Control Structure:

Sources of Earnings / Funds:

1. Source

- | | |
|--|--|
| <input type="checkbox"/> Home Remittance | <input type="checkbox"/> Export import proceeds Stock/Investment/FX Trading Business |
| <input type="checkbox"/> Income | <input type="checkbox"/> Salary income (Mention Employer Name & Contact Details) |
| <input type="checkbox"/> Local Trading | <input type="checkbox"/> Royalty Income Dividends |
| <input type="checkbox"/> Property | <input type="checkbox"/> Rent |
| <input type="checkbox"/> Others (Please Specify) | |



How was the amount required for the proposed transaction accumulated?	
Name of the bank and Jurisdiction from where the funds will be transferred?	
In whose name is the above account? If not in your name, how is the account owner related to you?	
In case of purchase by the Company, please provide Company's bank statement.	

Annual Income:

Purpose of Purchase:

Main Line of Business activities (For Sole Proprietor / Self-employed)

Counter Parties & Geographies:

- | | | |
|--|--|---|
| <input type="checkbox"/> Financial Institution | <input type="checkbox"/> Govt. Entity | <input type="checkbox"/> Partnership |
| <input type="checkbox"/> Limited Company | <input type="checkbox"/> NGO/NPO | <input type="checkbox"/> Proprietorship |
| <input type="checkbox"/> Self Employed | <input type="checkbox"/> Others (Please Specify) | |

Geographies involved (Places) of Counter Parties (To be Specified)

Politically Exposed Persons (PEP) means the holder of a public office position or prominent public function (e.g. head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior executive of a state-owned co-operation or an important political party official):

- ☐ Exposed ☐ Not Exposed

If exposed, please select relevant options:

- | | | |
|---|--|--|
| <input type="checkbox"/> Legislative | <input type="checkbox"/> Armed Forces Person | <input type="checkbox"/> Judiciary Executive |
| <input type="checkbox"/> Administrative | | |

➤ By way of Family member / Association with PEP, Family member / Associated person details to be mentioned.

In Case of Representative:

In case, the customer is represented by an authorized agent or representative or agent, or where customer is a legal person, the natural persons including Directors, Shareholders, Executive etc. who act on behalf of the customer to be mentioned and above-mentioned information to be provided in relation to these persons.



In Case of Joint Customer:

In the case of joint customers, the KYC form specified above will be filled in for all the joint Customers as if each of them is an individual customer.

DECLARATION:

I / We hereby consent that the personal information provided shall be reviewed and processed for the purpose of fulfilling the requirements of Federal Decree No. 20 of 2018 on Anti-Money Laundering and Combating Financing of Terrorism and Illegal Organizations (AML Law), the Cabinet Resolution No 10 of 2019, concerning the Implementation of the AML Law, and Cabinet Resolution No 58 of 2020 regarding Beneficial Owners procedures.

I / We acknowledge and understand that the information obtained through this form will be used to undertake the client due diligence in compliance with the regulatory requirements. Further, I / We acknowledge that based on the outcome of the client due diligence, the Firm at its sole discretion reserves the right not to proceed with the client onboarding without any liabilities whatsoever.

I / We hereby confirm that the above information provided to you is true and correct to the best of our knowledge.

I / We acknowledge that if the information provided is found to be false or misleading then the business relationship may be annulled anytime at your discretion. I/We hereby agree to provide any additional information/documentation that may be required.

DOCUMENT CHECKLIST**Section A. Required Documents (Mandatory)**

1. Emirates ID, Passport Copy, visa.
2. Trade License, Company registration, MOA, List of shareholders with shareholding % (if applicable).
3. Proof of address, e.g., a recent utility bill (not more than 3 months old), tenancy agreement, bank statement etc.
4. Salary Certificate

Section B. Additional Documents which may be requested

1. In the case of **crypto currency**, provide wallet details / statements.
2. Proof of Source of Funds / Wealth like Audited Financials, Bank Statement of past one (1) year, documents confirming sale of an asset, dividend, inheritance, bonus etc.

I / We confirm that all the information and documents provided herein are true and accurate.

By / On behalf of Customer:

Name:

Date:

Signatures:

By Company Representative

Name & Designation:

Date:

Signatures:

Note: In case the customer is outside UAE, only verifiable and officially registered digital signatures are acceptable.



APPENDIX – 5 AUTOMATED CUSTOMERS DUE DILLIGENCE FORM (CDD)

As the form concludes on specific questions and overall risk rating that is to be allocated to each client. Below table summarises different risk ratings and course of action to be followed.

Risk Rating	Risk	Course of Action
1 (One)	Low Risk	Proceed to accept the client
2 (Two)	Medium Risk	Exercise Professional Judgement While Accepting Client
3 (Three)	High Risk	Additionally Perform Enhanced Due Diligence
4 (Four)	Risk at Unacceptable Level	Reject the client

Internal Reference Number:

Client Name (Use Capital Letters)

Client Identification Number:

EID/PASSPORT Expiry Date (dd-mm-yyyy):

Is this a joint customer transaction?

Nature of Transaction:

Amount of Transaction:

If transaction is being undertaken jointly please fill separate forms for each individual?

****For Joint Customers, use separate CDD forms for each***

List of documents provided by the client during KYC
(Know Your Customer)

1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

Documents Requirement:

For CDD (Customer Due Diligence):

Documents to verify source & amount of investment	<input type="text"/>
Copy of Documents obtained	<input type="text"/>

Documents requirement for EDD (Enhanced Due Diligence)

Documents to verify Source of Wealth and individual's net worth	<input type="text"/>
Documents to verify source and amount of investment	<input type="text"/>
Copy of Documents Attached	<input type="text"/>



If the response to any of the statements in Section A is "Yes", the company shall NOT establish business relationship with the client.

SECTION A

Sr.	Statements	Response	Course of Action	Risk Rating
1	The client is unable to provide all the required information in the relevant forms.	No	Continue to Answer Next Statement	1
2	The required information obtained cannot be verified to independent and reliable documents.	No	Continue to Answer Next Statement	1
3	The client, beneficial owner of the client, person acting on behalf of the client, or connected party of the client matches the details in the following lists: (a) The "Lists of Designated Individuals and Entities" (b) The "Terrorist Alert List"; or (c) Any other similar lists and information required for screening purposes stipulated by relevant authorities in UAE including the Accounting and Corporate Regulatory Authority; and the exceptions cannot be disposed of satisfactorily.	No	Continue to Answer Next Statement	1
4	There is suspicion of money laundering and/or terrorist financing.	Yes	WARNING: DO NOT Establish Business Relationship with Client	4

Summarised Form (Only for the case of understanding)

Please note that for below are NOT to be accepted at all:

- Individuals, Entities, Crypto Wallets, Vessels etc forming part of sanctions list.
- Where required information is not provided.
- Where Information obtained cannot be verified to independent and reliable documents.
- There is suspicion of money laundering and/or terrorist financing.

Client/Customer, Country/Territory, Services/Transactions Risk Factors

Response to question in Section B, C and D will result in various course of actions. In case course of action for any of these state "DO not establish business relationship then client shall not establish business relationship, however the company shall fill full CDD form to evaluate if there are multiple instances which result in non-establishment of business relationship. For other responses, automated risk rating will be given after analysing responses from all sections.

SECTION B

CLIENT'S RISK FACTORS

Sr.	Statements	Response	Course of Action	Risk Rating
1	Is the client, any of the beneficial owner of the client or person acting on behalf of the client a Politically Exposed Person (PEP), family member of a PEP or close associate of a PEP? https://www.opensanctions.org/	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
2	The company has performed further screening of details of client, beneficial owner of the client, person acting on behalf of the client, or connected party of the client against the sanctions lists, and/or other third-party screening database. https://www.opensanctions.org/	Yes	WARNING: DO NOT Establish Business Relationship with Client	4
3	Against other information sources, for example, Google, Newspaper, Twitter etc. Are there adverse news or information arising?	Yes	Medium Risk, Exercise Professional Judgement	2
4	Is the client in a high-risk industry ? If client is a legal entity or Individual has shareholding in any such company: - Real estate brokers and agents. - Dealers of precious metals & precious stones. - Auditing or accounting firms. - Corporate services providers. Reference: Circular Number (3) of 2023 regarding Updated list of High Risk Jurisdictions	Yes	Medium Risk, Exercise Professional Judgement	2

5 & 6 applies only if:

5	Are the client's company accounts NOT updated?	Yes	Medium Risk, Exercise Professional Judgement	2
6	Does the client's shareholders and/or directors frequently change, and the changes are unaccounted for?	Yes	Medium Risk, Exercise Professional Judgement	2



SECTION C

SECTION C: COUNTRY / TERRORITY RISK FACTORS

Sr.	Statements	Response	Course of Action	Risk Rating
1	<p>Is the client, beneficial owner of the client or person acting on behalf of the client from or based in a country or jurisdiction in relation to which the FATF has called for <u>countermeasures</u>?</p> <p>The following would be applicable: -For Individual(s) clients -Nationality -Residential address</p> <p>For clients that are legal entities/clients that have ownership in company: -Country of Incorporation / registration -Registered address -Address of principal place of business</p> <p><i>*https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html (BLACK LIST: As of October 2023 Iran, Myanmar & Democratic People's Republic of Korea make up the Black List, please use the link above to access the updated list)</i></p>	No	Low Risk	1
2	<p>client from or based in a country or jurisdiction known to have <u>inadequate AML/CFT measures</u>?</p> <p>The following would be applicable: nationality, country of incorporation / registration, residential address, registered address, address of principal place of business.</p> <p><i>*https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html (GREY LIST: Please check updated list from the link above)</i></p>	Yes	Medium Risk, Exercise Professional Judgement	2

SECTION D

SERVICES / TRANSACTIONS RISK FACTORS

Sr.	Statements	Response	Course of Action	Risk Rating
1	Is the business relationship with the client established through online, postal or telephone, where <u>non-face-to-face approach</u> is used?	Yes	Medium Risk, Exercise Professional Judgement	2
2	Has the client given any instruction to perform a transaction (which may include cash) anonymously?	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
3	Has the client transferred any funds without the provision of underlying services or transactions?	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
4	Are there <u>unusual patterns of transactions</u> that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)?	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
5	Are there <u>unaccounted payments</u> received from unknown or un-associated third parties for services and/or transactions provided by the client?	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
6	Is there instruction from the client to make any <u>transaction on behalf of shell companies</u> with nominee shareholder(s) and/or director(s)?	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
7	<p>Does the client <u>set-up or purchase companies or business entities</u> that have <u>no obvious commercial purpose</u>?</p> <p>This would include:</p> <ul style="list-style-type: none"> • Multi-layer, multi-country, and complex group structures. • Setting up entities in UAE where there is no obvious commercial purpose, any other personal or economic connection to the client. 	Yes	High Risk: Additionally Perform Enhanced Due Diligence (EDD)	3
8	Is there any <u>divergence in the type, volume or frequency of transactions</u> expected in the course of the business relationship with the client?	Yes	Medium Risk, Exercise Professional Judgement	2



Risk Rating & Approval:

Question wise Risk Rating	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Section A	1	1	1	4	-	-	-	-
Section B	3	4	2	2	2	2	-	-
Section C	1	2	-	-	-	-	-	-
Section D	2	3	3	3	3	3	3	2

Course of Action:**RISK RATING****4 Reject the client**

Prepared by _____	
Signature:	
Name:	
Position:	
Date:	
Assessed by MLRO:	
Signature:	
Name:	
Position:	
Date:	
Approved by Owner:	
Signature:	
Name:	
Position:	
Date:	



SECTION E**Enhanced Due Diligence**

*Sources of Wealth: Indicates each source of wealth (including past sources) which contributed to your wealth (e.g. occupation, investments, inheritance, borrowings, etc); and estimated amounts generated from each source.

*Source of funds: Refers to the origin of the particular funds or other assets which are the subject of the establishment of company-client relations.

Sr. No	Source of Wealth (Total Wealth)	Total Amount AED	PEP Related AED	Verified by Documents
1				Yes
2				Yes
3				Yes
4				Yes

Sr. No	Source of Funds (Funds required to perform underlying transaction)	Total Amount AED	PEP Related AED	Verified by Documents
1				Yes
2				Yes
3				Yes
4				Yes

Source Of Wealth as a percentage of Wealth

#DIV/0!

#DIV/0!

EDD Risk Rating

Prepared by _____	
Signature:	
Name:	
Position:	
Date:	

Assesed by _____	
Signature:	
Name:	
Position:	
Date:	

Approved by _____	
Signature:	
Name:	
Position:	
Date:	



Attach Screen Shots from below sources to verify customer identity and to search across various platforms a

Sr Number	Source of Evidence	Attachment/Screen Shot
1	From UAE Local List	
2	From UN Consolidated List	
3	From OPENSANCTIONS.ORG (DataBase)	
4	From Google, Twitter, Facebook, Other Social Media Platforms (if other please specify)	

Application of Enhanced Due Diligence Form



This form applies to the following individuals where the company determines that enhanced customer due diligence is required:

- (a) Client (individual);
- (b) Beneficial owner of a company;
- (c) Where no individual can be identified as beneficial owner, the person having executive authority in a company; and
- (d) Any other individual the company determines to be necessary.

Situations where enhanced customer due diligence may be required include the above individuals identified as:

- (a) A foreign PEP, or his family members and close associates.
- (b) A high risk domestic PEP, or his family members and close associates.
- (c) A high risk international organization PEP, or his family members and close associates.
- (d) Individual belonging to country included in Black List.
- (e) Instruction to perform a transaction (which may include cash) anonymously
- (f) The client transferred any funds without the provision of underlying services or transactions
- (g) Unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank drafts etc.)
- (g) Unaccounted payments received from unknown or un-associated third parties
- (h) Where client gives instruction to make any transaction on behalf of shell companies with nominee shareholder(s) and/or director(s)
- (i) Set-up or purchase companies or business entities that have no obvious commercial purpose
- (j) Multi-layer, multi-country, and complex group structures.



	NAME	TITLE	SIGNATURE	DATE
Authoriser	Maia Barshiny	General Manager		14/11/2023
Authoriser	Shristi Chaudhary	MLRO		14/11/2023

Change History

Policy No.	Effective Date	Issuance Number	Last Review Date
001	14/11/2023		

