ارجي ريفاينري م.م.ح
RG REFINERY FZE

ANTI-MONEY LAUNDERING & COMBATING FINANCING OF TERRORISM POLICY

RG REFINERY FZE

Document Version Control			
Document Name: AML/CFT Policy (By the assistance of UAE Good Delivery Approved Auditors)			
Document Author:	Joel John	RGR Compliance Officer	
Reviewed by:	NM Shameem	RGR General Manager	
Approved by:	Mohammed Rafeeq Nandoli	RGR Owner	
Issue Date:	3rd September 2024		
Approved date:	6th September 2024		

ارجي ريفاينري (م.م.ح) COMPLIANCE APPROVED RG REFINERY (FZE)

Document last updated September 2024

Table of Contents

Definition of Terms 4

1. INTRODUCTION 7

2. PURPOSE 7

3. AML/ CFT LEGISLATIVE FRAMEWORK 8

3.1. The Financial Action Task Force (FATF) 8

3.2. The Ministry of Economy (MOE) AML/CFT Regulation and the UAE Good Delivery Framework 8

3.3. Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations 9

3.4. Cabinet Decision No. (10) of 2019 9

4. ROLES AND RESPONSIBILITIES 9

4.1. Responsibilities of the Compliance Officer 9

4.2. Responsibilities of the Senior Management 10

4.3. Responsibilities of the Employees 10

5. RISK ASSESSMENT 11

5.1. Identification of the Inherent Risk Factors for Precious Metals and Stones Sectors 11

6. KNOW-YOUR-CUSTOMER (KYC) 11

6.1. KYC Requirements for Individual Customers 12

6.2. KYC Requirements for Corporate Customers 13

6.3. Customer Risk Assessment 14

6.4. Simplified Due Diligence 15

6.5. Enhanced Due Diligence 15

Sanctions Screening 16

6.6. Politically Exposed Persons (PEP) 19

7. MONITORING OF CUSTOMER TRANSACTIONS / ACTIVITIES 19

8. SUSPICIOUS TRANSACTION REPORTING 21

9. TIPPING OFF AND CONFIDENTIALITY 23

10. TRAINING AND AWARENESS 23

11. RECORD KEEPING 25

11.1. Record Retention Policy 25

11.2. Record Destruction Policy 25

12. ACKNOWLEDGMENT 26

13. LIST OF APPENDICES 26

Foreword

It is the policy of RG REFINERY FZE to conduct its business in an honest and ethical manner. RG REFINERY FZE adheres to best practices with respect to the Anti Money Laundering & Combating Financing of Terrorism (**"AML/CFT"**) Policy, and therefore it has zero tolerance for Money Laundering & Financing of Terrorism activities, including related involvement, if any by employees, officers, directors, agents, consultants, suppliers, customers and contractors of RG REFINERY FZE.

The purpose of this AML/CFT Policy is to provide RG REFINERY FZE and its employees specific guidance relating to our legal and regulatory obligations to enforce measures to deter and detect money laundering and financing of terrorism activities. Because AML/CFT obligations are contained in several laws, amendments and regulations and as such laws, rules and regulations may have extra-territorial application, RG REFINERY FZE and its employees and associated persons are always required to adhere to all these requirements across all jurisdictions where RG REFINERY FZE may operate, even if such conduct might otherwise be permitted by the local law of a particular jurisdiction.

RG REFINERY FZE will take all appropriate action to ensure compliance with this AML/CFT Policy and applicable laws [Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations and the Cabinet Decision No. (10) of 2019, rules and regulations, which may include disciplinary action, like reporting of violations of laws, rules and regulations to appropriate regulatory authorities. RG REFINERY FZE is committed to continual improvement and this document represents our first step towards establishing, implementing and maintaining a robust Anti Money Laundering & Combating Financing of Terrorism management system.

Definition of Terms

Terms	Definitions
AML & CFT	Anti-Money Laundering (AML) refers to the policies, procedures and controls implemented by the company and other regulated entities to prevent, detect, and report money laundering activities. Countering the Financing of Terrorism (CFT) involves the measures taken to prevent and combat the provision, collection, or movement of funds intended to support terrorist activities.
Beneficial Owner	The natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a Transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement.
CDD	"Customer due diligence" is the process of identifying or verifying the information of a customer or Beneficial Owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it for the purposes of the Decretal-Law and this Decision.
Customer	An individual or entity that engages with the Company or a service provider. This includes buyers, sellers, miners, refiners, suppliers, and sub-suppliers.
DNFBPs	Designated Non-Financial Businesses and Professions (DNFBPs) Means Real estate agents & Dealers in precious metals. Dealers in precious stones. Lawyers, notaries, other independent legal professionals, and accountants.
FATF "Financial Action Task Force"	The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standards.
UAE FIU	United Arab Emirates Financial Intelligence Unit means the agency will collect raw transactional information and Suspicious activity reports (SAR) usually provided by banks and other entities as part of regulatory requirements.
Gold Bullion	Bullion means precious metal bars and coins (gold, silver, and platinum) that are designated for trading through their sale or purchase in units of ounces, kilograms and/or ten tolas and are considered high-quality precious metals, unless stated otherwise by the company, and comply to the minimum purity requirements of the Dubai Good Delivery (DGD) and London Good Delivery (LGD) standards.
Gold Ingot	A gold bar, also called gold bullion or gold ingot, is a quantity of refined metallic gold of any shape that is made by a bar producer meeting standard conditions of manufacture, labeling, and record keeping. Larger gold bars that are produced by pouring the molten metal into molds are called ingots.

Governance	Governance-related requirements are stipulated under AML/CFT Law No.20 of 2018, Article 16.1(d) and AML/CFT Cabinet Decision No. (10) of 2019, Article 4.2(a), 20, 21, 2 Term Definition 44.4 and AML/CFT guidance for Designated Nonfinancial Businesses and Professions (DNFBPs) issued by the Ministry of Economy (April 1, 2019), Article 8.
LLC	Limited Liability Company
LSM	Large-scale or medium-scale mining is governed by a framework of regulatory controls, permits and inspections and is subject to health, safety, social, environmental, closure and governance standards. Large-scale mining involves the payment of royalties and other taxes to governments in return for developing publicly owned mineral resources.
ML/TF	Money laundering is the process by which the financial proceeds of crime are disguised to conceal their illegal origin. Money laundering refers to activities designed to conceal or disguise the origin of the proceeds of crime (i.e., predicate offences) through processes that transform illegal inputs into legitimate outputs. The proceeds of crimes such as theft, fraud, corruption, and drug trafficking are made to look like the fruits of honest activity - for example, by being converted into legitimate bank accounts, real estate, or luxury goods. Terrorism Financing is the illegal smuggling of money to terrorist organizations. Terrorist financing is often linked to money laundering and is often conducted across international borders. Terrorist financing involves the collection and processing of funds from both legal and illegal sources to provide terrorists with the resources to conduct their attacks. While the phenomena differ in key respects, they often seek to exploit the same vulnerabilities that allow an inappropriate degree of anonymity and non-transparency in the conduct of transactions.
Non-Resident	A natural person who is a non-UAE national and who does not have a legal right to work and live in the UAE
Occasional Transaction	Any transaction other than a transaction conducted during an established Business Relationship.
OECD Guidance	Organization for Economic Co-operation and Development Means the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas
Politically exposed persons (PEP)	"Politically exposed persons" - When individuals are elected to prominent political positions or assigned high-profile public roles, they should be categorized as politically exposed persons (PEPs) to reflect their increased risk of involvement in money laundering or terrorism financing.
Proliferation Financing (PF)	This means providing funds or financial services for the transfer and export of nuclear, chemical, or biological weapons; their means of delivery and related materials.
Recycled Gold and/or Precious Metals	Recycled Gold means gold and/or precious metals that have been previously refined, such as end-user, post-consumer and investment gold and/or precious metals and products containing gold and/or precious metals, as well as scrap and waste metals and materials generated during refining and product manufacturing, including recovered materials from industrial recovery, that are returned to a refiner or other downstream intermediate processor to start a new life cycle as "recycled gold". The

	origin of the recycled gold and/or precious metals is considered to be the point in the supply chain where the gold and/or precious metals are returned to the refiner or other downstream intermediate processor or recycler; assay samples are excluded from this category and are outside the scope of verification if the member is able to do so.
Resident	For this questionnaire, a resident is a natural person who is a UAE national/non-UAE national and who does have a legal right to work and live in the UAE.
Suspicious Activity Report (SAR)	A report that details the activity or transactions that raised suspicion.
Suspicious transaction	A suspicious transaction is a transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction.
Suspicious Transaction Report (SAR)	A Suspicious Transaction Report (STR) is a report that is required to be filed with the relevant UAE Financial Intelligence Unit (UAE FIU) when they detect activity that might indicate money laundering, terrorist financing, or other illegal conduct.
Trade-based money laundering (TBML)	Trade-Based Money Laundering takes advantage of the complexity of trade systems, most prominently in international contexts where the involvement of multiple parties and jurisdictions make AML checks and customer due diligence processes more difficult. TBML primarily involves the import and export of goods and the exploitation of a variety of cross-border trade finance instruments.
Targeted Financial Sanctions (TFS)	Targeted Financial Sanctions are measures for asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of specified entities/ designated persons who are being sanctioned.
Transaction	Transaction is defined under Article 1 of the Cabinet Decision No. (10) Of 2019 "Transaction: All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation."

1. INTRODUCTION

Money laundering, including trade-based money laundering, terrorism and proliferation financing has far-reaching consequences for a country's financial system and economy. With these crimes becoming increasingly cross-border in nature, companies must equip themselves to protect the integrity of their financial systems and must also be prepared to deal with any abuses that are encountered.

To achieve this, we must have a sound and robust legal framework, which empowers RG Refinery (FZE) and lays out the obligations of all parties concerned.
A properly functioning anti-money laundering policy, procedures and controls can help protect revenue and combat crime throughout the value chain from the time a precious mineral is first mined to the time of sale in the market.

2. PURPOSE

The purpose of this AML/CFT policy (the "policy") is to set out the responsibilities of RG REFINERY (FZE) (or the "company") and all employees of the company in fulfilling its' commitment to prevent, detect and respond to money laundering and terrorist financing. In this policy, the company refers to the fulfilment of AML/CFT Obligations defined in the Cabinet Decision No. (10) of 2019, MOE Anti-Money Laundering Regulation/Supplemental Guidance for Dealers in Precious Metals and Stones and Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions.

The company will ensure that all its staff are aware of the Policy and its contents, including the penalty for non-compliance, and will not tolerate any violation of this Policy by its staff/management.
The provisions, procedures and controls detailed in the below sections are mandatory and shall apply to:

- All the employees regardless of their function or location of work.
- All customers, including buyers, sellers, miners, refiners, suppliers (including sub-suppliers), and gold and precious metals trading companies.

The following principles will apply in the context of the company's Anti Money Laundering & Combating Financing of Terrorism ("AML & CFT") Policy:

(a) It is our policy to conduct all our business in an honest and ethical manner. We take a zero-tolerance approach to money laundering and terrorism financing, and we are very committed to acting professionally, fairly and with integrity in all our business dealings and relationships whenever we operate.

(b) It is our best practice objective that those we do business with take a similar zero-tolerance approach to money laundering and terrorism financing.

(c) Other bound by the laws of the United Arab Emirates ("UAE") in respect of our conduct both at home and abroad and businesses that deal with Gold, Silver and other precious metals are required to meet the regulatory requirements set out in the Anti-Money Laundering and Combating Financing of Terrorism policy.

(d) Assess the risks and apply a risk-based approach to Customer Due Diligence, by collecting enough information to be satisfied that the underlying transactions are legitimate and implement a robust recordkeeping and reporting system to ensure AML compliance.

3. AML/ CFT LEGISLATIVE FRAMEWORK

3.1. The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) leads global action to tackle money laundering. FATF provide a framework in their guidance document titled "Risk-Based Approach (RBA) Guidance for Precious Metals and Stones Dealers". It defines 'Dealers in Precious Metals' as a broad range of actors, from miners to intermediate buyers and brokers, to those who cut, polish or refine precious metals, to retail sellers and finally, those operating in the secondary and scrap markets. Six of FATF's 40 recommendations are directly relevant to the 'Precious Metals' sector:

a) FATF R.1 – Assessing the risks and applying a risk-based approach.
b) FATF R.22 – Implement Customer Due Diligence measures to know their customers and suppliers and to collect enough information to be satisfied that the transaction is legitimate.
c) FATF R.23 – Prepare and send Suspicious Transaction Reports for further analysis, upon suspicion that the funds are proceeds of criminal activity, and/or related to terrorist financing.
d) FATF R.28 – Dealers in precious minerals should be regulated and monitored for compliance with the AML/CFT requirements, namely Customer Due Diligence (CDD), recordkeeping, and reporting.
e) FATF R.32 – Measures should be in place to detect the cross-border transportation of cash and bearer negotiable instruments, with precious metals considered as bearer negotiable instruments.
f) FATF R.34 – Guidelines and feedback should be provided to precious metals dealers by competent authorities including their supervisors.

3.2. The Ministry of Economy (MOE) AML/CFT Regulation and the UAE Good Delivery Framework

In the UAE, the overarching guidance is set out in the MOE AML/CFT Guidelines for DNFBPs and Supplemental Guidance for Dealers in Precious Metals and Stones.

The Ministry of Economy (MOE) has recently introduced Due Diligence Regulations for Responsible Sourcing of Gold that necessitate all UAE refiners to undergo a comprehensive Supply Chain Audit annually starting from 2023. This regulation is in line with the UAE Good Delivery (UAEGD) Rules and is designed to integrate with existing AML/CFT legislation. The goal is to enhance the responsible sourcing of gold and ease the compliance burden on refiners.

The company is committed to performing the appropriate due diligence as required by the regulatory bodies in the UAE.

3.3. Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations

This decree-law forms the cornerstone of the UAE's AML/CFT legal framework. It outlines the responsibilities of businesses, including gold refineries, to implement AML/CFT measures such as customer due diligence, suspicious transaction reporting, and record-keeping.

The law mandates the identification of beneficial owners, enhanced due diligence for high-risk customers, and cooperation with authorities in investigations.

3.4. Cabinet Decision No. (10) of 2019

This regulation provides detailed guidelines for implementing the AML/CFT decree-law, including the responsibilities of DNFBPs, which include gold refineries.

It includes specific measures for risk assessment, internal controls, reporting obligations, and international cooperation.

4. ROLES AND RESPONSIBILITIES

4.1. Responsibilities of the Compliance Officer

RG REFINERY (FZE) will always employ a full-time experienced Compliance Officer ("CO") who will be responsible for the Compliance function of the organization. The CO will have the following duties:

- Solely responsible for creating and implementing the AML/CFT compliance program and ensuring compliance with AML/CFT Laws, Regulations, Notices, Standards, and international laws.
- Establishing and maintaining appropriate AML/CFT policies, procedures, processes, and controls in relation to the business of the company.
- Ensuring compliance by the company employees with the provisions of AML/CFT Guidelines, its implementing rules and regulations and the company's AML/ CFT Policy.
- Disseminating to the Board of Directors, Officers, and all employees any circulars, resolutions, instructions, and policies issued by the UAE Regulatory Agencies in all matters relating to the prevention of Money Laundering and combatting of Financing of Terrorism and Financing Illegal Organization's.
- Liaising between the company and UAE Regulatory Agencies in matters relating to compliance with the provision of AML/CFT Compliance Guidelines and its implementing rules and regulations.
- Preparing and submitting to UAE Regulatory Authorities authored reports on the company's compliance with the provisions of the AML/CFT Compliance.
- Creating a gap analysis document on existing AML/CFT Procedures and current Laws, Regulations, Notices, and Standards of the UAE to determine the extent of the level of compliance and recommend actions if required.
- Designing the compliance training program and providing regular training for employees and other staff members at the company, particularly when any laws change, or new risk is identified.
- Assessing all internal suspicious transaction alerts from employees and investigating the matter along with presenting the findings of all the suspicious activities/transactions to the UAE FIU.

- Performing more extensive, due diligence for high-risk customers and including proactive monitoring for suspicious types of activities.
- Submitting Suspicious Transaction Reports to the UAE FIU in a timely manner through the GoAML system.
- Interface with UAE FIU's integrated enquiry management system, which is a platform to exchange specific requests and related correspondence.
- Maintaining all necessary CDD, transactions, STR and staff training records for the required period of five years.

4.2. Responsibilities of the Senior Management

The Senior Management will have the following duties:

- Implementing a robust AML/CFT policy and procedures across all units.
- Ensuring that the company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- Approving the overall business risk assessment for the company.
- Reviewing the compliance report along with high-risk areas.
- Oversight of Internal Audit reports and ensuring the observations detailed in the report are addressed in a timely manner.
- Ensuring that all employees of the organisation are being trained on AML/CFT.
- Ensuring that all reports to the regulator (UAE FIU) are thoroughly reviewed and delivered accurately and on time.
- Ensuring that the compliance team is provided with adequate and qualified resources to effectively carry out their duties.
- Approving the AML/CFT policy and reviewing compliance issues raised by the CO.

4.3. Responsibilities of the Employees

The employees will have the following duties:

- Performing due diligence on new and existing customers, including identification and verification of all KYC documentation.
- Monitoring customer transactions for unusual or suspicious activity.
- Reporting any suspicious activities/transactions identified to the CO and maintain the confidentiality of any identified suspicious activities/transactions.
- Maintaining accurate and complete records of all transactions as required.
- Participating in AML/CFT training programs to stay informed of the relevant ML & TF risks and understand the company's AML/CFT policies and procedures.

5. RISK ASSESSMENT

At RG REFINERY (FZE), we understand, assess, and identify the money laundering and terrorism financing risks associated with our everyday business on a day-to-day basis. We implement a sound ML/TF risk assessment methodology to suit the size, nature, and complexity of our daily business. We employ additional parameters which are relevant to the nature, size, and complexity of our business before we enter a new business relationship and to identify and assess ML/TF Risks. A risk-based approach is one of the most effective ways to protect against ML and TF. It is essential to understand that certain risks associated with the various elements of a customer profile may be indicative of potential criminal activity, such as geographic and jurisdictional issues, business and product types, distribution channels and transaction types and amounts.

The company is committed to taking appropriate steps to identify, assess, understand and mitigate all risks related to Money Laundering and Terrorism Financing.

Per the FATF's 'Recommendation 1 - Assessing the risks and applying a risk-based approach' is a crucial element of the implementation of the risk-based approach.

5.1. Identification of the Inherent Risk Factors for Precious Metals and Stones Sectors

The inherent risk factors associated with the precious metals and stones sector for the purpose of conducting a risk-based assessment are listed below.

- **Customer Risk:** Involves the risk associated with different types of customers for example: high-net-worth individuals, politically exposed persons (PEPs), non-resident customers, sanctioned individuals and large transactions being conducted by unestablished customers.
- **Product Risk:** Involves the risk associated with the product or service the customer intends to utilize, as well as the company's role, which should be clearly defined from the outset. Due to their nature, the precious metals attract ML and TF activities.
- **Geographic Risk:** Involves risks from operating in or dealing with entities from high-risk jurisdictions, sanctioned countries, cross-border transactions, countries identified as Conflict-affected and High-Risk Areas (CAHRAs) and areas prone to trade-based money laundering.
- **Transaction Risk:** Involves the risk associated with the nature and characteristics of individual transactions such as large or irregular transactions, and cash-intensive transactions.
- **Delivery Channel Risk:** A delivery channel is a medium that can be used to obtain a product or service, or through which transactions can be conducted. This involves risk associated with the delivery channels such as conducting cash settlement, payments via third parties or payments via unknown online platforms, etc.

6. KNOW-YOUR-CUSTOMER (KYC)

The identification and verification of a customer's identity is a fundamental component of an effective ML/TF risk management and mitigation programme.

The company maintains clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk than average risk. Before accepting a potential customer, KYC and due diligence procedures are followed, by examining factors such as customers' background, country of origin, public or high-profile position, linked accounts, business activities or other risk indicators.

KYC shall be conducted in accordance with the mandatory customer KYC form, which details the required corporate/individual information to be obtained, the relevant questionnaire and the key documents required.

- Corporate KYC Form *(Refer to **Appendix 1**)*
- Individual Members of a Corporate Customer KYC Form *(Refer to **Appendix 2**)*

According to Article 6 of the Cabinet Decision No. (10) of 2019, the company will conduct KYC and CDD procedures when:

- Establishing a new business relationship.
- Carrying out occasional transactions above the applicable designated threshold.
- There is suspicion of money laundering or terrorist financing.
- There are doubts about the veracity or adaptability of the previously obtained customer identification data.
- It is necessary to obtain additional information from existing customers based on the conduct of the account.
- There are changes to signatories, mandate holders, beneficial owners, and other relevant key personnel.

If the customer is unable to comply with the above-mentioned requirements, the company will adopt the following courses of action as required:

- Not to proceed with the business relations or perform the transaction.
- Terminate the business relationship.
- Consider filling a suspicious transactions report in relation to the customer.

When conducting the KYC process, there will be no reliance on third-party information or "hearsay". For applicants introduced to the company by a third party, the CO will ensure to perform all identification, verification and KYC procedures.
The company will ensure that KYC procedures are a fundamental practice to protect the company from fraud and losses resulting from illegal funds and transactions.

6.1. KYC Requirements for Individual Customers

The company will obtain from all individual applicants the following information:

- Applicant's full name (as per passport)

- Date and place of birth.
- Nationality.
- Passport Number.
- National Identity Document (Emirates ID, for UAE nationals / Residents)
- Physical Address (residential and business / home country and UAE)
- Contact details.
- Previous personal / business activities / occupation (type and volume)
- Anticipated type and volume of company's activities.
- Bank reference and introductory letter; and
- Source of funds.
- Declaration regarding Beneficial Ownership, which is the person who has ultimate ownership of entitlement over funds.
- Whether the customer is a Politically Exposed Person (PEP) or a close associate of a PEP.

6.2. KYC Requirements for Corporate Customers

Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound up or terminated. In case of doubt as to the veracity of the corporation or the identity of its directors and/or officers, or the business or its partners, a search or inquiry with the relevant Supervising Authority/Regulatory Agency shall be made.

The company shall obtain from all corporate applicants the following KYC information

- Incorporation name.
- Shareholders (in case the applicant company is non-publicly traded)
- Ultimate beneficial owners (the Beneficial Owner shall be whoever person that ultimately owns or controls, whether directly through a chain of ownership or control or by other means of control such as the right to appoint or dismiss the majority of its directors, 25% or more of the shares or more of the voting rights in the Legal Person);
- Managers (the person having day-to-day control of the company if not a shareholder/partner)
- Authorized Signatories.
- Passport copies of all shareholders, ultimate beneficial owners, managers, and signatories.
- National Identity document of shareholders, ultimate beneficial owner, managers, signatories (Emirates ID, if the applicant is a resident/citizen of UAE)
- Memorandum and Articles of Association.
- Power of Attorney (if applicable)
- Country of origin / UAE physical address (if applicable)
- Contact details.
- Previous business activities (type and volume)
- Anticipated type and volume of activities.
- Last two years audited financial statements.
- Source of funds; and

- Bank reference and introductory letter.

For companies or businesses registered outside the UAE, comparable documents are to be obtained, duly authenticated by the UAE Embassy where said the embassy is located.

If significant changes to the company structure or ownership occur subsequently, or suspicions arise because of a change in the payment profile as reflected in a company account, further checks are to be made on the identification of the new owners.

Additionally, the company will re-review the KYC information whenever certain triggers occur, such as:

- Significant changes in the customer's business structure or ownership.
- Changes in the customer's transaction patterns that are inconsistent with their established profile.
- New regulatory requirements or updates to AML/CFT laws.
- Receipt of adverse information about the customer, such as being listed on a sanctions list.

6.3. Customer Risk Assessment,

All potential customers will be subjected to a Customer Risk Assessment and each customer's risk rating will be calculated and recorded in the ***Customer Risk Assessment Tool*** *(Refer to* ***Appendix 3)****.* The Customer Risk Assessment Tool will decide on the Overall Customer Risk Rating and accordingly, the level of due diligence required will be ascertained.

Due diligence procedures performed will be commensurate with the risk level associated with the customer.

- **High-risk customers** will be subjected to enhanced levels of due diligence that are detailed in Section 6.5. titled 'Enhanced Due Diligence'.
- **Medium-risk customers** will be subjected to a standard level of due diligence. For a medium-risk customer, the company will include additional steps to mitigate the medium level of risk identified for their customers.
- **Low-risk customers** may be subjected to Simplified Due Diligence procedures detailed in Section 6.4. The Company will ensure that it continues to meet the minimum legal obligations.

The application of risk-based CDD measures is comprised of several components, in keeping with the customer's ML/TF risk classification and the specific risk indicators identified. These components include, but are not limited to, the following categories:

- Identification of the customer, beneficial owners, or controlling persons; and the verification of the identity based on documents, data or information from reliable and independent sources.
- Background screening of the customer, beneficial owners, or controlling persons, to screen for the applicability of targeted or other international financial sanctions, and,

particularly in higher risk situations, to identify any potentially adverse information such as criminal history.

- Obtaining an understanding of the intended purpose and nature of the business relationship, and, in the case of legal persons or arrangements, an understanding of the nature of the customer's business and its ownership and control structure.

6.4. Simplified Due Diligence

A low-risk Customer will present a lower-than-normal risk of involvement in money laundering or financing of illegal activities.

Simplified customer due diligence measures (SDD) are applied to the customers identified as low risk. SDD involves a more lenient application of certain aspects of customer due diligence measures.
For identified low-risk customers, SDD may result in the following adjustment to the due diligence procedures:

- A reduction in verification requirements for customer or Beneficial Owner identification.
- Fewer detailed inquiries regarding the purpose of the business relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions.
- Less frequent review and updating of customer due diligence information; and
- Completion of the verification of customer identity after the establishment of a business relationship.

Listed companies are exempted from the obligation to identify and verify the identities of shareholders, partners, or beneficial owners of a legal entity, provided that:

- The necessary identity information can be obtained from reliable public domain sources such as corporate registries, websites of relevant ministries, etc; and
- The customer, or the owner holding the controlling interest of the customer, is a company listed on a regulated stock exchange subject to adequate disclosure and transparency requirements related to Beneficial Ownership; or when the customer, or the owner holding the controlling interest of a legal entity customer, is the majority- held subsidiary of such a listed company.

6.5. Enhanced Due Diligence

A high-risk customer will present a higher-than-normal potential risk of involvement in money laundering or financing of illegal activities.

To mitigate the increased risks associated with High-Risk Customers, it will be necessary to consider the application of a level of enhanced due diligence for those customers. The company's Senior Management with the consultation of the CO will determine whether the level of risk is acceptable.

The company will perform Enhanced Due Diligence in the following scenarios:

- Customer entities incorporated in high-risk countries or CAHRAs (Conflict-affected and High-Risk Areas).
- Politically Exposed Persons (PEPs) and close associates of PEPs.
- If the customer/ transaction is suspicious or unusual.
- Customers identified as high-risk during the Customer Risk Assessment.
- When dealing with high-risk products.
- Dealing with customers that are highly cash dependent.

As the reasons for designation as high-risk will vary from customer to customer, the nature and level of enhancement will need to be determined separately as and when high-risk customers are identified.

All high-risk customers must be approved in writing by the Compliance Officer and the Senior Management.

The additional documents required from high-risk customers include the following:

- Audited Financial Statement
- Tax Return
- Bank Statements
- Bank Reference Letter
- Dubai Good Delivery / LBMA (London Bullion Market Association) Certificates
- Independent Assurance Report
- Business Profile (including business dealings and any investments)

Furthermore, when dealing with customers who are highly cash-dependent, additional documents are required:

- Source of Funds Declaration
- Transaction Justification
- Declaration of Cash Transaction
- Customer's internal cash handling policies, if any.

Sanctions Screening

Sanctions Screening is a crucial component of the company's AML procedures that involves checking individuals, entities, and transactions against various sanctions lists to ensure compliance with national and international regulatory requirements.

The company will take all required steps to ensure that all customers with whom a business relationship is established have been 'screened' for hits on the relevant sanction lists, such as:

- United Nations Security Council (UNSC)

- UAE (Local, Terrorist List)
- The Office of Foreign Assets Control (OFAC)
- Her Majesty's Treasury Department – UK (HMT)
- European Union Sanctions (EU)

The company will ensure compliance with the applicable sanction's laws in every jurisdiction that it may choose to trade or operate in.

The company's Sanctions Compliance Program includes a customer screening control. The company uses Win Guard AML tool to perform the screening.

The control is dependent on a reliable matching engine that compares data from internal and external sources against each other, to detect similarities that indicate a match. Once a match has been identified, an alert is sent to the CO.

The CO will review and assess whether the alert indicates a 'true match' or a 'false positive' On identification of a true match, necessary measures are applied such as blocking the transaction/freezing of funds and filing an STR and/or a Partial Name Match Report within 24 hours (from the time receiving the 'true match' alert) to the UAE FIU through the GoAML platform[1] (*refer to the footnote for instructions on submitting*).

6.5.1. Sanction List Management

Sanction List Management is the process of managing, maintaining and updating lists of individuals, entities, countries, and other entities that are subject to sanctions or restrictions imposed by government and international bodies.

The first step in the sanctions list management process is to determine and prioritise the lists deemed relevant for screening. These may be externally sourced lists from third-party list providers or lists from regulatory websites (e.g. OFAC, UN, EU, etc.). The selection of lists depends on various factors such as the type of customers, products offered, and nature of the business.

The use of external third parties for sourcing and maintaining regulatory sanction lists should have a formal process for reconciling its third party-provided lists with regulatory lists, to ensure completeness.

On the other hand, relying on regulatory website sanction lists requires a process that consolidates data from various formats and sources. In addition, some customers will be included in more than one list, so it is necessary to remove duplicates as not doing so may cause an alert to be generated twice. In such cases, the company should consider implementing a sanction list management system to clean, parse and format the list data to improve matching accuracy and reduce the number of false positives.

The company should consider establishing and maintaining a "Whitelist" of customer names or other data elements that have already been flagged and cleared through customer screening by the company as false positives. These "Whitelists" may be used to

[1] https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=e23d1292-e656-46b3-8866-5cf75e240c12

improve the process related to customer screening by leveraging the results of past screening reports and reducing the number of false positives.

The company should document the procedures for managing and periodically reviewing and updating these "Whitelists" to account for the possibility that customers on a whitelist may later become sanctioned persons.

6.5.2. Integrated Enquiry Management System ("IEMS")

The CBUAE has introduced a new system called the Integrated Enquiry Management System ("IEMS") which is a platform designed to manage and streamline the exchange of enquiries and information requests between various authorities and entities[2] (*Refer to the footnote for more information regarding the IEMS platform).*

Through this platform, the UAE FIU can request information and documents from the company, aiming to provide results to law enforcement authorities more efficiently.

6.5.3. Sanction Screening Testing (Thematic Review)

A thematic review in sanction screening testing is an in-depth examination of the systems and processes used by organisations to screen for sanctions. This type of review focuses on specific themes or areas of interest, such as the effectiveness and efficiency of the screening systems, compliance with regulatory requirements, and the identification of best practices.

The sanction screening testing through thematic reviews is to ensure that the company's sanction screening processes are robust, effective, and aligned with the regulatory requirements. The company should conduct periodic and focused reviews to identify potential gaps, weaknesses, or areas for improvement.

The review involves testing of the company's customer screening system by:

- **Fuzzy Logic Matching**: Manipulated data are recorded that have been deliberately altered to test customer screening system fuzzy logic matching capabilities.
- **Clean ID**: Customer records that do not appear on any sanction lists. These are included to see the customer screening system's tendency to pick up false positives and represent real-life customer data.
- **Alert Management:** Assessing how the customer screening system handles and prioritises alerts.
- **False Positives/Negatives Analysis:** Assessing the rate of false positives and negatives to evaluate the customer screening system's accuracy.
- **List Matching:** Verifying that the customer screening system correctly matches names and other identifiers against sanctions lists.

[2] https://www.uaefiu.gov.ae/media/jtdnttby/integrated-enquiry-management-system.pdf

6.6. Politically Exposed Persons (PEP)

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective.

The Cabinet Decision No. (10) of 2019 defines PEPs as natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of State or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:

(a) Direct family members (Of the PEP, who are spouses, children, spouses of children, and parents).
(b) Associates who are known to be close to the PEP, which include:

- Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP.
- Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

In addition to undertaking the normal customer due diligence procedures, appropriate screening tools are to be put in place to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP.

The overall risk is increased considerably when a PEP is in a high-risk country. If a PEP is identified, the company will:

- Assign a rating of high-risk to the customer.
- Obtain Senior Management approval before establishing a Business Relationship with a PEP, or before continuing an existing one.
- Conduct enhanced due diligence and be vigilant in monitoring the business relationship.
- Ensure reasonable measures will be taken to establish the source of wealth and source of funds.

7. MONITORING OF CUSTOMER TRANSACTIONS / ACTIVITIES

With regards to established business relationships, the company is obliged to undertake ongoing supervision for its customers' activity, including the transactions executed throughout the course of the relationship to ensure that they are consistent with the information, types of activity and risk profiles of the customers.

The company follows a manual transaction monitoring process. The CO manually reviews the daily transaction logs, focusing on key red flags/indicators such as large cash transactions and/or transactions involving high-risk jurisdictions, etc.

Additionally, the company should give more emphasis on monitoring transactions that equal or exceed AED 55,000 (as per Cabinet Decision No. 10 or 2019, Articles 3 and 6). This threshold applies to both single transactions and multiple related transactions with the same customer.

In the case of customers or business relationships identified as high-risk, the company will evaluate the specifics of the transactions examined in relation to the customer's due diligence information or profile and obtain sufficient information on the customers involved to determine whether the transactions appear to be 'Normal', 'Reasonable', or 'Legitimate':

- **Normal -** Whether the transactions are typical for the customer, for the other parties involved, and for similar types of customers.
- **Reasonable** - Whether the transactions have a clear rationale and are compatible with the types of activities that the customer are usually engaged in.
- **Legitimate -** Whether the customer is permitted to engage in such transactions, such as when specific licenses, permits, or official authorizations are required).

If the transaction does not appear to be Normal, Reasonable or Legitimate then further review will be conducted to identify any potential red flags or indicators of a suspicious transactions/ activities.

Upon identification of a suspicious transaction, the matter is escalated to the CO for further investigation. A report detailing the suspicious transaction, along with all relevant documentation and findings, is compiled for review.

The CO conducts a thorough investigation, which may involve contacting the customer for additional information and based on the findings, a decision is made regarding the suspicious nature of the transaction. If the transaction is confirmed as suspicious, the CO will obtain approval from the Senior Management and files a Suspicious Transaction Report (STR) to the UAE FIU.

Accurately identifying and assessing the ML and TF risks of customer or business relationship is critical for appropriately managing these risks.

The following are list of possible or potential red flags or indicators of suspicious activities/ transactions.

The Business Relationship or Customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant, unable or refuse to explain:
    - Their business activity and corporate history.
    - The identify 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 (third parties located in foreign jurisdictions).

- Is a person or business seeking to perform transactions without providing a relevant license.
- Has no clarity of how the customer transports the merchandise it has bought.
- Is a designated individual or an organization (i.e., on a sanction list).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists of terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Is a politically exposed person or is associated with a person who is politically exposed?
- Who does not provide appropriate documentation of payment or origins for high-risk artisanal and small-scale gold?
- That has a director(s) 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 authorized the transaction.
- Appears to be acting according to instructions of unknown or inappropriate person(s).

Customer Transactions:

- Uses considerable sum of cash, without an adequate explanation as to its source or purpose.
- Who conducts an unusual number or frequency of transactions in a brief period.
- That requests payment arrangements which appear to be unusually or unnecessarily complex or confusing (for example, unusual deposits or instalment arrangements, or payments in several different forms), or which involve a third party.
- That provides identification, records or documentation which is falsified or forged.
- That appears structured to avoid the cash reporting threshold.
- Involves any attempt by a physical person or controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to: over-or-under invoicing of goods or services, over-or-under shipments [example: false entries on bills of lading]; or multiple trading of the same goods or services).
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the customer.

The presence of one or more of the indicators does not necessarily mean that a transaction involves ML/TF, however, it is an indication that further investigation and more stringent risk assessment should be undertaken.

8. SUSPICIOUS TRANSACTION REPORTING

The company will institute a system of mandatory reporting of suspicious transactions pursuant to Cabinet Decision No. (10) of 2019 [Articles 13 and 16]. The company will report any suspicious

activities or transactions (SARs/STRs) to the UAE Financial Intelligence Unit (UAE FIU) through the GoAML system.

Where any employee or personnel, director or officer of the company suspects that the customer has engaged in any of the predicate crimes, the matter must be promptly reported to the CO.

If there are reasonable grounds to suspect that the customer has engaged in unlawful activity, the CO, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the UAE FIU as Suspicious Activity/Transactions unless the CO records an opinion that such reasonable grounds do not exist.

The 5W1H (Who, what, Where, When, Why and How) method can be effectively applied to Suspicious Transaction Reporting (STR) to ensure a thorough and comprehensive analysis.

- **Who –** To understand the individuals or entities who are involved in conducting the transaction.
- **What** – Clearly describing what has occurred which involves detailing the nature of the transaction, the amount involved, the type of account used, and any anomalies or irregularities observed.
- **When –** The timing of the transaction that encompasses the date, time and the sequence and frequency of the transaction.
- **Why** – Exploring the reasons behind a transaction helps in understanding its legitimacy. This involves analysing the stated purpose of the transaction versus the observed behaviour and background information on the parties involved. Discrepancies between the purpose and the transaction pattern can highlight potential suspicious activities.
- **How –** Describing how the transaction was conducted provides a complete picture.

The company is expected to file an STR/SAR within a maximum of 35 business days from the date of alert of a suspicious transaction/activity.

Once a STR is submitted, the system generates a confirmation receipt, which includes a unique reference number for tracking purposes. The UAE FIU reviews the submitted STR and sends an acknowledgement to the company confirming that the report has been received and is being reviewed.

The GoAML portal allows the CO to check the status of the submitted reports. The CO can log in to the portal and navigate to the "My Reports" section to view the status of the STRs.

The UAE FIU may request additional information or clarification regarding the submitted STR. These requests are communicated through the GoAML portal, and the CO can respond directly within the system.

Once the UAE FIU has completed its review, the final disposition of the STR is updated in the GoAML system. The company is notified of the outcome, which could include further investigation, closure, or other actions.

The company will maintain a register of all suspicious transactions that have been brought to the attention of the CO, including transactions that are not reported to the UAE FIU. This register shall contain details of the date on which the report is made, the person who the report to the CO and the information sufficient to identify the relevant papers related to the said report.

The company acknowledges that failure to report suspicious transactions, whether intentionally or by gross negligence, is a federal crime. Any person who fails to perform their statutory obligations is liable to a fine and/or imprisonment or both.

9. TIPPING OFF AND CONFIDENTIALITY

Tipping off occurs when a person discloses information to a customer or a third party that is likely to prejudice an investigation into ML or TF.

The employees of the company will not warn or share the information with the concerned individual or entity about the information being reported to or investigated by the relevant authority.

The company will enforce strict disciplinary action against any employee who deviates from this policy.

All company staff should note that he/she must not inform any customer/colleague that the customer is being scrutinised for possible involvement in suspicious activity related to ML.

If the employee reasonably believes that performing CDD will tip off a customer or potential customer, the employee may choose not to pursue that process. If the employee decides to do so then he/she must promptly notify the CO, who will decide whether a SAR/STR should be filed.

When reporting suspicious transactions to the UAE FIU, the Company will maintain confidentiality about both the information being reported and the act of reporting itself. The company will make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

According to Article 25 of the UAE Federal Decree No. 20 of 2018, anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the competent authorities is punishable by a penalty of imprisonment for no less than six months and/or a fine of no less than AED 100,000 and no more than AED 500,000.

10. TRAINING AND AWARENESS

To maintain effective AML/CFT compliance in the company, all our employees should be aware of this policy and appropriately trained to identify and report suspicious activity.

The CO should provide or organise the provision of annual AML/CFT training to all relevant employees.

The regular training received by employees will cover the AML Policy, the KYC procedures, the UAE and international regulations, and the procedure for the identification and reporting of suspicious transactions. The company's policy is to provide all relevant employees with AML training within Thirty (30) days of joining the company.

Employees include customer contact employees, operational staff, and senior management.

In RG REFINERY (FZE), we ensure that the CO must undergo a minimum of forty-eight (48) hours of external training in AML/CFT every year as a part of the Continuous Professional Development Program.

- Mandatory induction training on AML/CFT for all new hires.
- To upgrade the Product Knowledge of Front line / Operations & Support Services.
- For all other employees, refresher training at regular intervals

The Topics covered by AML/CFT training have been tailored as per the roles of the employees. The Training material incorporates all the requirements of MOE. Furthermore, the CO will maintain a record of attendance of all conducted training sessions.

11. RECORD KEEPING

The company will maintain detailed records (including electronic and physical data and documents) for all customer transactions, as well as a variety of record types and documents associated with their ML/TF risk assessment and mitigation measures, as specified in the relevant provisions of the AML-CFT Decision.

Required to maintain the records in an organized fashion to permit data analysis and the tracking of financial transactions, and to make the records available to the Competent Authorities immediately upon request.

11.1. Record Retention Policy

The following documents shall be considered as the company's AML/CFT Documents:

- All customers' documentation as provided in the KYC checklist and/or correspondences, including the documents obtained during CDD and/or EDD.
- All documentation relating to a suspicious activity report concerning a customer or applicant together with any response or follow-up.
- Records of AML/CFT training sessions attended by the company's staff, officers and their affiliates, the dates, content and attendees.
- Records of minutes of meetings of the AML/CFT Committee, including the details of all decisions taken by the committee.
- Records of all AML/CFT decisions taken by the Senior Management.

The following document retention periods shall be followed:

- All records of transactions of customers, especially customer identification records, shall be maintained and safely stored, physically or in electronic form, in an easily accessible place for five (5) years from the date of the transaction.
- With respect to closed accounts, the records on customer identification, account files and business correspondence shall be preserved and safely stored for at least five (5) years from the date of closure.

If the records relate to an ongoing investigation or transactions that have been the subject of disclosure, they shall be retained beyond the stipulated retention period until it is confirmed by the UAE FIU that the case has been closed.

11.2. Record Destruction Policy

- Records must be deleted/destroyed when they have reached the conclusion of the retention period.
- Records should be disposed of in a manner which preserves the confidentiality of the record(s).
- Records that have no retention requirement, and/or duplicate records, must be deleted/destroyed unless approval to preserve said record is obtained from the Senior Management.

12. ACKNOWLEDGMENT

All representatives (employees, suppliers, and sub-suppliers) are required to acknowledge their understanding and acceptance of this policy on a yearly basis and at the time of onboarding. Acknowledgement forms will be collected and retained by the Compliance Department.

13. LIST OF APPENDICES

Appendix No.	Description
1	KYC Form (Corporate)
2	KYC Form (Individual)
3	Customer Risk Assessment Tool
4	Inherent Risk Assessment