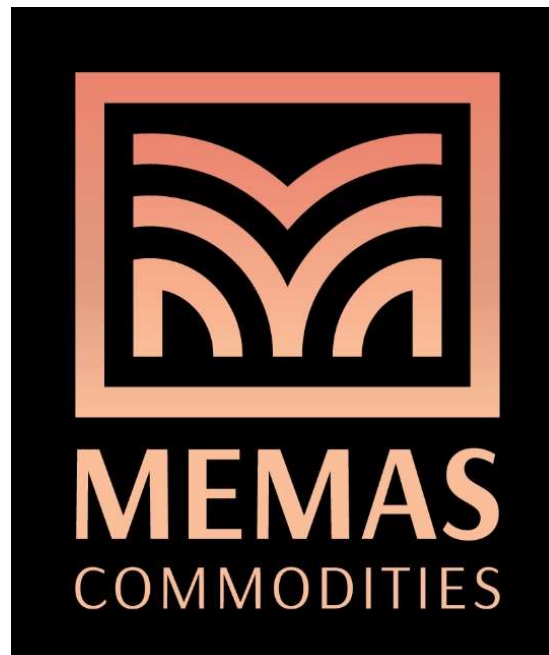


MEMAS COMMODITIES DMCC

Policy Rule Book

Version Rev 04.05B.2021



Statement of Corporate Philosophy

Customer orientation, security, profitability, growth, competitiveness, hard work, and attention to detail are the pillars of economic success and are the basis on which we run the company.

We are committed to the highest ethical standards in the formulation and pursuit of our objectives —"our word is our bond". The company does not engage in transactions that are doubtful and/or lack transparency. It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorism or criminal activities. All employees of the company are required to commit to maintaining the highest possible ethical standards of business conduct and adhere strictly to the Company's policies and procedures.

The integrity and commitment of each staff member ensure that the company provides fast, efficient, customer-friendly, and discreet services.

- Memas motivates staff members to exceptional levels of achievement through teamwork, creating an enjoyable working environment, and rewarding staff fairly according to their performance.
- Memas believes in equal opportunity for all staff members, male and female, and in the principle of providing a 'fair day's pay for a fair day's work". We are an attractive, caring and fair-minded employer.
- Memas" operates rigorously according to customers' requirements and above-named market potential, always bearing in mind the need to observe all legal and regulatory rules and regulations.

The basic criteria are for Memas to produce maximum benefit for its customers by offering a competitive range of tailor-made physical precious metals products and services while at the same time optimizing the returns to all stakeholders in Memas.

This is achieved by ensuring that " Memas" is known by its' clients for:

- Efficiency, speed and friendliness
- Error- free customer service any complaints must be settled quickly, fairly and amicably.
- High levels of security and discretion.
- Exceptionally personal style of customer contact and reaction to the customers' needs.

1. INTRODUCTION

Memas Commodities DMCC (the "Company") is committed to maintain the highest standards of Anti- Money Laundering (AML), Countering Financing of Terrorism (CFT) and Illegal organizations. In addition, Memas ensures to take adequate measure and prohibit its dealing with the Sanctioned individuals or entities. The Managing Director and all employees of Memas are committed to protect Memas and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

2. REGULATORY GUIDELINES

Memas being a dealer in the precious stones and is considered as Dealers in Precious Metal and Stones (DPMS) within the purview of Designated Non-Financial Business and Profession (DNFBPs) and is regulated by the UAE Ministry of Economy. The requirements mentioned in this policy are based on the MENA FATF Recommendations and National Risk Assessment and regulations in the UAE applicable for Dealers in Precious Metal and Stones namely:

Local regulations/circulars/guidelines:

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
- 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.
- Cabinet Decision No. (10) of 2019, Concerning the Implementing Regulation of Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
- Cabinet Resolution No. 20 for 2019 concerning the UAE list of terrorists and 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.
- Cabinet Decision No. (58) of 2020 Regulating the Beneficiary Owner Procedure.
- Cabinet resolution 74 of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions.
- Cabinet Decision No (16) of 2021 regarding the Unified List of the Violations and Administrative Fines for the Said Violations of Measures to Combat Money Laundering and Terrorism Financing.
- Cabinet Resolution No. (24) of 2022 amending some provisions of Cabinet Resolution No. (10) of 2019 regarding the executive regulations of Federal Decree-Law No. (20) of 2018 regarding countering money laundering crimes and combating the financing of terrorism and the financing of illegal organizations.
- Ministry of Economy - Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations Guidelines for Designated Non-Financial Businesses and Professions and Supplemental Guidance for Dealers in Precious Metal and Stones.
- Ministry of Economy Circulars for DNFBPs and Dealers in precious Metal and stones.
- Relevant Circulars and amendments as issued from time to time including those from the UAE Executive office for control and non-proliferation.

International legislative frameworks

- The United Nation: The UN is the international organization with the broadest range of membership. The UN actively operates a program to fight money laundering; the Global Programme against Money Laundering (GPML), which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).
- The Financial Action Task Force (FATF): The Financial Action Task Force (FATF) sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.
- Middle East and North Africa Financial Action Task Force (MENAFATF): MENAFATF was established in 2004 as a FATF Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with those standards. The UAE is one of the founding members of MENA FATF.

3. PRINCIPLES

The key principles underlying the AML, CFT and Sanctions policy is to:

- Maintain the confidentiality and integrity of the customer data.
- Meet the UAE regulatory, statutory, and legislative requirements on AML/CFT/Sanctions.
- Report and investigate all suspected breaches and suspicious cases to the FIU and/or Ministry of Economy.
- Conduct AML & Sanction Training & awareness to all employees (permanent & contract employees).
- Design appropriate controls and procedures to support the implementation of this policy.
- Continually improve AML and Sanction related controls through implementation of corrective and preventive actions.

4. OBJECTIVE AND SCOPE

To ensure to protect Memas and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes by dealing in the precious stone transactions with the suppliers, its customer or associated party to the transaction. This policy applies to all staff, business relationship, counterparty and customers of Memas whether in the physical working environment or remote working environment. The policies also apply to the suppliers of the precious Metals and require them to ensure that they adopt practices, relevant jurisdictional regime and/or equivalent standards to combat the money laundering and financing of terrorism and prohibit dealing or engaging with sanction individual or entity.

5. STAGES OF MONEY LAUNDERING

There are three stages of Money Laundering:

- **Placement:** During placement, “dirty” money derived from criminal activities is placed in the financial system whether such money arises from the purchase or sale of the precious metal or stone.
- **Layering:** To conceal the illegal origin of the placed funds and thereby make them more useful to criminals, the funds must be moved, dispersed, and disguised. Layering is the process of disguising the source of the funds through layers of financial transactions.
- **Integration:** Once the funds are layered and can no longer be traced back to their criminal origins, they are integrated into the financial system and now appear “clean” and available for use by criminals. If layering has been successful, integration places the laundered money back into the economy and financial system in such a way that they appear as clean and legitimate.

6. RESPONSIBILITIES

- The owner of Memas is responsible for ensuring the policy development, approval, implementation, maintenance, and endorsement.
- All employees of the Memas are responsible to read, understand and adhere to this policy in their day-to-day activities.
- The Compliance Officer is responsible to carry out periodic check on the state of implementation of the policy.
- Memas through its compliance officer is required to maintain adequate records related to those covered transactions, and report suspicious transactions, among others.

- Notwithstanding the duties of the Compliance Officer, the ultimate responsibility for proper supervision, reporting, and compliance pursuant to AML/CFT Compliance policy, or as amended, its revised implementing rules and regulations shall rest with Memas and its owner.

7. DEFINITIONS

- **Money Laundering**

Money laundering is the term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

- **Terrorist Financing**

Terrorist financing refers to activities that provide financing or financial support to terrorists. Transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering. It may involve funds raised from legitimate sources, such as personal donations, profits from businesses and charitable organizations.

- **Sanctions**

Sanctions are political and economic decisions that are a part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations, either to protect national security interests or to protect international law and defend against threats to international peace and security.

8. GOVERNANCE

Memas may appoint a Compliance Officer as required under the AML Regulations or any additional person as required from time to time to dispense with the Regulatory obligations and ensure enforcement and oversight of AML/Sanction process and control in the business.

9. AML, CFT & SANCTIONS CONTROL MEASURES

AML, CFT and Sanctions control measures includes but is not limited to the below:

9.1 AML/CFT Business Risk Assessment

The AML/CFT business risk assessment is a critical component Memas perform the risk assessment to identify money laundering and financing of terrorism risks across all business lines and processes. Based on a risk-based approach, Memas to periodic AML Risk assessment to identify and understand risks specific to its trading activity.

The AML risk profile is determined after identifying and documenting the risks inherent to the Memas trading activity and its roles in the supply chain but not limited to:

- Customer risk,
- Geographic risk,
- Channel risk,
- Products risks and
- Transactions risks

9.2 Know your customers (KYC), Identity and Verification

Memas implement KYC FORM to ensure all category of customers (including but not limited to natural or legal persons or legal structures) are subject to adequate identification and monitoring measures.

Verifying the identity of customers and true beneficial owners using reliable, independent sources, and keeping a record of all reference documents used to verify their identity is critical to any business relationship. Additionally, Memas would corroborate with reference to independent sources in identifying true beneficial owner.

Customers/Business Relationships should be made aware of Memas explicit policy that business transactions will not be conducted with applicants who fail to provide competent evidence of their identity, but without derogating from Memas obligations to report suspicious transactions. Where initial verification fails to identify the applicant or give rise to suspicious that the information provided is false, additional verification measures should be undertaken to determine whether to proceed with the business. Details of the additional verifications are to be recorded.

Memas will maintain customer accounts only in the name of the account holder. It shall not open or keep anonymous accounts, fictitious names accounts, incorrect name accounts and similar accounts. All documents as such requested in the due diligence process would be consider and classified as true copies of the original. The KYC FORM should capture the Customer due diligence requirements:

❖ CUSTOMER DUE DILIGENCE (CDD)

All information and documents must be collected before entering into business relationship:

NATURAL PERSONS:

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

Documents required

- The passport and identity card (Emirates ID) of individual customers must be checked and a certified copy thereof must be maintained.
- List of non-exhaustive documents for example Driving license, Recent Utility bill, rates or council tax bill, Statement from a regulated bank, building society or credit card company, mortgage statement issued from a regulated lender, Salary Certificate from customer's current employer on a company letter head signed by the authorized person with company stamp, Tenancy Contract or Rental Agreement.
- The Company shall request individual applicants who present only photocopies of identifications and other documents to produce or show the original documents for verification purposes. The prospective customers shall be interviewed personally.

The following checks shall be instituted for non-face-to-face prospective applicants and customer:

- Telephone contact with the applicant at an independently verified home or business number.
- Subject to the applicant's consent, telephone verification of the applicant's employment with the employer's personnel department at a listed business number;
- Income or salary details appearing on recent bank statements, income tax returns or any other document evidencing income or compensation;
- Confirmation of the address through an exchange of correspondence or by other appropriate methods;
- An initial deposit drawn on another financial institution regulated by the central bank of uae will provide additional assurance as to identity.

CORPORATES

- Incorporated name
- Shareholders and or controlling interest (in case applicant company being non-publicly traded);
- Ultimate beneficial owners (in case applicant company is not publicly-traded);
- Managers Details
- Signatories Details
- Country of origin / UAE physical address (if applicable);
- Contact details
- Anticipated type and volume of activities;
- Audited financial statements
- Source of funds; and Source of Wealth

Document Required

- Valid Registration Certificate, Trade & Regulatory License showing registration details.
- Valid VAT Certificate.
- Copy of the Memorandum of Association and Articles of Association showing the renewal date and all the partners including their shareholding pattern.
- Tenancy Contract of the Office to validate the names and addresses and official presence of the business
- Audited Financial Copy of the Firm to validate the source of wealth and source of funds.or
- Statement from a regulated bank,
- Certified copies of the identification document of Ultimate Beneficial owners, Corporate Organisation Chart etc
- Certified copies of the identification document of authorized signatories.
- Self Attested copy of Tenancy Contract /utility bill of the UBO and shareholders name and residential address to validate the Residency Status.
- As for public shareholding companies, the names and addresses of the Chairman, members of the Board of Directors and shareholders whose holdings are in excess of 5% each.
- As for companies where the ownership has an involment of Trust, we would require a copy of the Trust Deed,and Identifaction document of the Trustee (Nominal and Benficial).
- Any additional documents as necessary for placement of any specific risks or carrying out additional diligence. List of non-exhaustive documents such as Recent Company Utility Bill

TRUSTEE NOMINEE OR FIDUCIARY ACCOUNTS

Memas shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. Memas will obtain satisfactory evidence of the identity of such agents and authorized signatories, and the nature of their trustee or nominee capacity and duties.

Where the Compliance officer or Memas staff entertains doubts as to whether the trustee, nominee or agent is being used as a dummy in circumvention of existing laws, it shall immediately make further inquiries to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, the Memas shall consider whether to proceed with the business, bearing in mind the “Know-Your-Customer” principle.

Memas does not deal with shell companies or illegal organization or sanction individual or entities by UAE Sanctioned List or the UNSCR Consolidated List.

❖ Enhanced Due Diligence (EDD)

In addition to the CDD, Enhanced due diligence is required for the High-risk customers including Politically Exposed Persons (PEPs) or in cases where the compliance has requested to perform enhanced due diligence as case may be. In ensuring carrying out enhanced due diligence Memas would:

- Increase scrutiny and will implement higher standards of verification and documentation from reliable and independent sources with regard to customer identity;
- Carry out more detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer’s business, the customer’s source of funds and source of wealth, and the purpose of individual transactions;
- Increase supervision of the Business Relationship, including the requirement for owner approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.
- EDD should also be applied where the Red flags has been identified (Refer Appendix 1 for list of Red Flags). In doing so Memas should ensure that it take reasonable measures to obtain adequate, substantiated, information about the customer, commensurate with the level of the risks identified.

Natural Persons/Individuals

- Obtain the information source of wealth and source of fund and verify by obtaining the Last three-month/Six-month Bank statements based on the risk assessment.
- Tax assessment documents or any other official correspondence issued by the central or local govt.
- Banking references;
- Domicile/ Residency Status
- Description of the customer’s primary trade area and whether international transactions are expected to be routine;
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
- Explanations for changes in business activity

Corporates

- Obtain the Source of Fund used in the transaction and verify using Audited Annual report/Financial Statement the annual income, Turnover etc. for the last three years.
- Obtain the name of the bank that the customer or the beneficiary deals with.
- Banking references;
- Domicile and Residency Status of the UBO , Shareholder and Director.
- Description of the customer's primary trade area and whether international transactions are expected to be routine;
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and

Compliance Officer has full discretion to request for any additional documentation to establish the identification of the Customer, Ultimate Beneficial Owner and/or the Source of Funds and the business relationship non-involvement into any conflict activity.

❖ Simplified Due Diligence (SDD)

Simplified due diligence is required if a customer is:

- Customer is from a Low Risk Country
- Customers has well established Source of Funds
- In case of listed company where such information is available from the third-party sources such as audited financial statement of the listed company on their website or in case of legal entity beneficial owner where the customer is holding the controlling interest of the legal entity listed on the stock exchange.
- Cases that are internally assessed and documented for simplified due diligence from time to time.

9.3 Sanction, PEP and Adverse Media Screening

All business relationship be its sales or purchases, irrespective of the size of transaction or the method of payment should undergo screening against the Sanction Lists. In doing so, the Memas may utilize the off the shelf subscription-based database, publicly available UAE local Terrorist list or UNSCR Consolidated list, and third-party screening tools to identify any adverse information including association with the PEPs or with crimes.

All our approved customers and suppliers would be listed for ongoing screening on our Screening Tool.

Memas does not conduct any business relationship/transaction that are on the UAE Cabinet blacklist or on Call for Action jurisdictions and Sanctioned jurisdictions. In compliance with UN Security Council resolution No. 1730/2006 and pursuant to UAE Federal Law No. 7 of 2014, the UAE publishes the National Sanctions Blacklist containing the names of individuals and entities identified as terrorist and associated with proliferation of weapons of mass destruction

(We also utilized the list obtained from Overview on UN Consolidated Sanctions List and National List of Terrorists | Committee for goods & material subjected to import & export (uaecic.gov.ae). Memas Strictly does not deal with such Entities or Individuals.

9.4 Acceptable Payments; Currency and Cash Equivalent Instruments

- **Cash Transactions:**
Memas does not accept any form of cash transactions.
- **Wire transfer/Credit Card Payment/Other Mode Cheque:**
All payment through this mode are subject to the Customer Due-Diligence and Enhanced Due-Diligence requirements based on Risk Categorization and mandatory Transactional Screening.
- **Payment in form of Precious Metal:**
All payment originating in form of precious Metal or stone or in form or exchange transaction will be subject to the Enhanced Due Diligence Review for CDD and Supply Chain.
- **All mode of payment by third parties:**
Memas does not accept or makes any form of Third-party Payments
- **Payment in form of Digital Assets/Crypto Currencies/NFT**
Memas does not accept any payment in form of the crypto or digital currency.

9.5 RISK RATING

RISK ASSESSMENT AND MITIGATION POLICY AND PROCEDURE

Memas Risk Assessment Policy is based on FATF and Ministry of Economy-UAE, guidance on the risk-based approach to combating money laundering and terrorist financing.

The Policy is the guiding principle to the effective implementation of the AML/CFT legislation at Memas, this policy is used to identify, assess, and understand the ML/TF risks to which they are exposed, and implement the most appropriate mitigation measures.

The Policy requires, Memas to identify, assess, and understand the ML/TF risks to which its exposed to, and implement the most appropriate mitigation measures. At Memas we understand Assessing this risk is, one of the most important steps in creating a good AML/CFT compliance program and will enable Memas to focus our resources where the risks are higher.

Memas has used a Risk-Based Approach to AML/CFT means that Memas should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. This will require an understanding of the ML/TF risk faced by the sector and the specific products and services, customer base, the capacity in which customers are operating, jurisdictions in which they operate, and the effectiveness of risk controls put in place.

Memas has included an assessment of the exposure of the business to money laundering risks from the Following:

1. **Business-wide Risks**
2. **Customer Risk**
3. **Customer Due Diligence Procedures and Risk**

Assessing Business-Wide Risks

An important first step in applying an RBA is to identify, assess and understand the ML/FT risks by way of a business-wide ML/FT risk assessment. The purpose of an ML/FT business risk assessment is to improve the effectiveness of ML/FT risk management, by identifying the inherent ML/FT risks faced by the enterprise, determining how these risks are effectively mitigated through internal policies, procedures and controls, and establishing the residual ML/FT risks and any gaps in the controls that should be addressed.

The first step of conducting an ML/TF business risk assessment for Memas is to identify, assess and understand the inherent ML/FT risks (i.e., the risks that a Memas is exposed to if there were no control measures in place to mitigate them) across all business lines and processes with respect to the following risk factors: customers, products, services and transactions, delivery channels, geographic locations, and any other risk factors.

The Factors that are considered in Business Risk Assessment are as follows

1. Customer-Related Risk
2. Geographic -Related Risk
3. Product and service-Related Risk
4. Channel-Related Risks
5. Transaction-Related Risks

a) CUSTOMER-RELATED RISK

The factors that are taken into the risks arising from customers are as follows

- target markets
- size of customer base
- business model and strength of a relationship
- Complexity and transparency of business ownership
- Regulation and supervision
- Association and Linkage

b) GEOGRAPHIC RISK

This factor assesses the risk from countries where the business is conducted and where the customers are based and should consider

- Regulatory / Supervisory framework of the countries where customers are based
- Risk Rating of the country where the customer/ supplier is incorporated on the Know your country risk rating
- Applicability of International Sanctions on the country where the company is incorporated. (UN, UAE and OFAC, UKHTM and EU)
- Consistency with the customer's profile

c) PRODUCT AND SERVICE-RELATED RISK

Under this Factor, we would assess the scope for use of the product offered for money laundering and should consider

- If the product (Gold) is associated with any existing money laundering typologies.
- Complexity of product or service that could be exploited for money laundering.
- Transparency and transferability related to the ownership of products
- Size and value of products offered and how those impact the money laundering risks.

d) CHANNEL-RELATED RISKS

These Factors assess the different channels used by the business for acquiring and management of customer relationships and conducting transactions.

- Mode of Delivery of the Product
- Number of Parties Involved in the Delivery of the Product
- Complete Documentation for the products delivered

e) TRANSACTION-RELATED RISK

These Factors assess the different Transactions used by the business for acquiring and management of customer relationships and conducting transactions.

- Volume of Cash Involved in The Transaction
- Third Party Payment Risk
- Mode of Payment Requested by the supplier and customer
- Country where the payments are requested to be made or made from.
- Unclear source of Funds for the Transactions

1. Customer Risk Assessment

Memas in order to assess the risk associated with each customer has classified the Risk category into the following:

- 1) **Low-Risk Customers and Suppliers**
- 2) **Medium -Risk Customers and Suppliers**
- 3) **High-Risk Customers and Suppliers**
- 4) **Prohibited Customers and Suppliers**

1. Low-Risk Customers and Suppliers

This classification categorizes the customer based on the factors such as customers who have:

- provided all the kyc documentation that is required to review all the details that is associated with the customer/supplier along with the ownership details and nature of the business.
- These customers have had long-standing business relationships with the Memas. The ownership structure is not complex.
- These customers have a regulatory and supervisory framework in the countries that they are incorporated in.
- The Risk Rating of the Country which these customers and Suppliers are incorporated are considered a Low Risk country by Know your country and FATF Risk Rating. These customers and suppliers are incorporated in countries that have no sanctions and are not in the FATF Grey List that require additional supervision.
- These companies are regulated and certified by Independent organizations such as LBMA, RJC and UAE Good Delivery.
- These customers have product size is less than 5 Kg per shipment, and they have provided the source of funds and source of wealth to make the purchase or sale of the products, Transparency and transferability related to the ownership of products is well established.

- The companies have a very transparent Mode of Delivery and has secured third party Logistics partners (like Brink, G4S, Transguard) ,involved in the supply of the product.
- These companies have No cash transaction involved all the payments are made and received through bank transfers
- The payment are not made to any related party or third party, the payment is made into the customer/ suppliers own bank account.
- These customers have no Multi Level of ownership, and UBO are from Low Risk countries and are not a PEP or associated to a PEP.
- These customers have no Hit during the screening (Sanction, PEP and Adverse Media).
- These customers have well-established AML and CFT Policies and Sourcing Policy

The course of Action:

A Standard Due Diligence will be conducted on Low-Risk Customers, by the Compliance Assistant Manager, who will review and conduct basic screening of the Customer/ Supplier and shareholders who would be placed under Ongoing Screening. These customers can be approved by the compliance Assistant Manager, after conducting Standard Due Diligence.

2. Medium -Risk Customers and Suppliers

This classification categorizes the customer based on the factors such as customers who have the following factors.

- Customer who has provided all the KYC documentation that is required to review all the details that are associated with the customer/supplier along with the ownership details and nature of the business.
- These customers have had long-standing business relationships with the Memas. The ownership structure is not complex.
- These customers have a regulatory and supervisory framework in the countries in that they are incorporated.
- The Risk Rating of the Country in which these customers and Suppliers are incorporated are considered a Medium Risk country by Know your country and FATF Risk Rating.
- These customers and suppliers are incorporated in countries that have no sanctions and are not on the FATF Grey List which requires additional supervision.
- These companies are regulated and certified by Independent organizations such as LBMA, RJC and UAE Good Delivery.
- These customers have a product size is less than 10-25 Kg per shipment, and they have provided the source of funds and source of wealth to make the purchase or sale of the products, Transparency and transferability related to the ownership of products are well established.
- The companies have a very transparent Mode of Delivery and have no third party involved in the supply of the product.
- These companies have Less than 10% cash transaction involved, and 90% of the payments are made and received through bank transfers
- The payment is not made to any related party or third party, the payment is made into the customer/supplier's own bank account.
- These customers have no Multi Level of ownership, and UBOs are from Medium-Risk countries.
- Local (United Arab Emirates) PEP are classified into this Category.

- The Supplier who is sourcing metal from medium Risk Country where the AML and Corruption are at medium levels.
- These customers have no Hit during the screening (Sanction, PEP and Adverse Media).
- These customers have well-established AML and CFT Policies and Sourcing policies.

The course of Action:

A Standard Due Diligence will be conducted on Low-Risk Customers, by the Compliance Assistant Manager, who will review and conduct basic screening of the Customer/ Supplier and shareholders who would be placed under Ongoing Screening. These customers can be approved by the compliance Assistant Manager, after conducting Standard Due Diligence. These customers will be reviewed on a Annual Bases.

3. High-Risk Customers

This classification categorizes the customer based on the factors such as customers who have the following Traits.

- Customer who has provided the basic KYC documentation that is required to review all the details that are associated with the customer/supplier along with the ownership details and nature of the business.
- These customers do not have a long-standing business relationship with the Memas and who any customer who has been in the business for less than one Year.
- The ownership structure is complex and has multiple levels of ownership of the company.
- These customers have very less regulatory and supervisory frameworks in the countries in which they are incorporated and countries that they operate in.
- The Risk Rating of the Country in which these customers and Suppliers are incorporated are considered as High-Risk country by Know your country and FATF Risk Rating.
- These customers and suppliers are incorporated in countries that are on the FATF Grey List which requires additional supervision.
- These Suppliers are involved in sourcing metal from directly from the mines, hence they are exposed to the high probability of Bribery, Corruption and Environment Abuse hence they are categorized as High Risk.
- These companies have large-scale shipment.
- These Companies have
- These companies are not regulated and certified by Independent organizations.
- These companies actively use Hand Carry and Air Cargo for their delivery and also use authorized third parties for the delivery of Metals.
- These companies have Less than 25% cash transactions involved, and 75% of the payments are made and received through bank transfers.
- The payment is not made to any related party or third party, the payment is made into the customer/supplier's own bank account.
- These customers have Multi Levels of ownership, and UBOs are from High -Risk countries or Sanctioned countries but are residents in Non-Sanctioned countries and have been living there for a period more than 3 years.

- International PEP from Low-Risk Countries and PEP's who have no Adverse Media against them are listed in this category.
- These customers have Potential Hits during the screening (Sanction, PEP and Adverse Media) but are found not to be a True Match.
- These customers have AML and CFT Policies and Sourcing policies.

The course of Action:

Compliance Manager would conduct an EDD review and conduct Enhanced screening of the Customer/ Supplier and shareholders, once approved these customers would be placed under Ongoing Screening. For these customers' all their transactions will be subjected to screening, the compliance manager will conduct a Monthly review of their overall activity to ensure the Risks are Mitigated.

Prohibited Category:

Any customer or supplier would be categorized as Prohibited if they fall under the below category.

- Any company or Shareholder registered in any Sanctioned country, the UBO is Residents of Sanctioned Countries or Countries that are listed in Conflict-Affected and High-Risk Areas or Operating from these areas.
- Is a foreign pep from a High-Risk Country and PEP who have adverse media Information.
- Is a restricted or sanctioned person on an official authority watch list.
- Where payment is made in form of precious metal and stones or equivalent form.
- Where business relationships and transactions are involved from Sanctioned jurisdictions.
- Person/country; located in a Conflict-Affected high-risk country; or is connected to the extraction industry, for instance, the extraction of natural resources such as gas, oil, diamonds, gold (and other precious metal), and wildlife (e.g., ivory trading) from CAHRA
- Has a complex ownership structure, making it difficult to identify the owners and controllers or know where funds are coming from or going.
- Is a charity or a 'not-for-profit organization (NPO) –terrorists may exploit charities to move funds, provide logistical support, encourage terrorist recruitment, or support other terrorist groups.
- Customers /Supplier and Shareholders who have been convicted for AML, Bribery, Smuggling, Human Rights Abuse, Human Trafficking etc.
- Customer so are not willing to provide KYC Documents to validate the Ownership of the firm.
- Customers who request payment to be made and received in form of cryptocurrency.
- Customers and suppliers who use shell banks and shell companies.
- Company or shareholder has been listed or associated with Terrorist List.
- Supplier who do not have proof of Tax Payment to the government for their shipment.
- Customer / Suppliers who do not have Valid Trade License, Export License and Mining License.
- Customer who have their company incorporated in a Black Listed country (Iran and Democratic Republic of Korea).
- Customer and Supplier who are Multiple Third party involved in Supply Chain.
- Companies who insist on conducting only cash-based transaction.
- Companies and Shareholders who have been True Match Hit during screening for (PEP, Sanctions and Adverse Media info).

The course of Action:

Compliance Manager would conduct review and Review and Straight away Reject these Customer and Suppliers at the time of on boarding. If its and existing customer, the staff will bring the concerns to the compliance manager who will conduct a review and would be reporting to the component authority via GO AML and conduct necessary actions as required by the regulator and Exist the relationship with the customer at the earliest.

A. Ongoing Screening:

All customer categories are subject to be ongoing screening for Sanction, PEP and Adverse media information A periodically risk-based review is carried out to ensure that customer-related data or information is kept up to date. This required periodic screening of the customer's transaction for high risk. In case of any unusual transaction or suspicious transaction or activity please follow the instruction on reporting as prescribed in the Policy.

B. High Risk Call for Action and Gray List by FATF

Memas does not deal with the High-Risk Call for Action countries (Refer FATF High-Risk Countries). During the course of business relationship if any transaction is originating from, routed through or destined to high risk jurisdictions "Call for action" as well as any financial or non-financial engagement involving an individual or entity hailing from (by virtue of nationality, residency, place of incorporation) a country classified as a 'High-Risk Jurisdiction subject to a Call for Action' by FATF (list available via link on NAMLCFTC's website -High Risk Countries) should be mandatorily reported as per Reporting requirements. Compliance officer shall determine to report such a transaction to FIU in appropriate form.

The list of Jurisdictions under Increased Monitoring (the Gray List), shall be adopted along with the requirements to implement procedures by DNFBPs that may include enhanced due diligence measures.

Memas shall continuously monitor the black list and gray list of FATF and take measure accordingly.

To refer to the Black and Gray list please visit the following National Committee website:

<https://www.namlcftc.gov.ae/ar/>.

C. Unusual Transactions, Suspicious Transaction and Suspicious Activity Reporting (SAR/STR)

Memas shall establish indicators through which crimes involving money laundering and terrorist financing can be suspected and appropriate enhanced due diligence and reporting requirement can be dispensed with. Refer Appendix 1 for non- exhaustive Suspicious activity Red Flag.

Internal Reporting

If any staff come across any suspicion or have reasonable ground to suspect that the transaction or the activity during the screening, the business relationship, counterparty or the customer represent all or some form of proceed or suspicion of their relationship to the crime or that they will be used regardless of the value shall be referred/reported to the Compliance Officer. In case of PEP, High Risk jurisdiction, all relationship should be signed by the Compliance officer and owner of the Memas.

External Reporting

Where it is sufficient that the transaction or the activity is suspicious in nature the Compliance team shall determine reporting of suspicious transactions and activities reports (STR / SAR), and to provide any additional information concerning these reports, and to update such indicators on ongoing basis, in addition to keeping a permanent update on relevant developments related to types, patterns and methods of money laundering and terrorist financing. Post the submission of the stated report, the reporting entity must wait for three working days before executing such transaction(s) unless it receives feedback from FIU with any advice or objection pertaining to the reported transaction(s).

In the absence of any response from the UAE FIU within three working days, the Compliance Officer based on the risk assessment of the case shall reserve the discretion to approve or deny the case. All business rejection cases by Compliance should be backed by the Memas owner. Tipping off is a punishable offence and is not permitted.

Memas shall make sure its Compliance Officer is registered to the Go AML Portal for direct reporting of Unusual/STR and SARs.

(Refer Appendix 2 on more info on Go AML Portal).

D. Politically Exposed Person (PEP) Screening

PEP refers to Politically exposed person. Natural persons who are or have been entrusted with prominent public function in the state or any their foreign country such as Head of the Government, Senior Politicians, State Government officials, judicial or military officials, senior executive managers or state owned corporations, and senior officials of political parties and person who are, or have been entrusted with the management of an international Organization or any prominent function within such an Organization including Direct Family members of PEP or Associates known to be close to Associates.

Enhance Due Diligence measures should be applied in case of business relationship, Counterparty or PEP has been identified as PEP Memas Owner's/ Compliance Mangers approval is must prior to proceeding based on risk assessment on all PEP cases. In doing so Memas should be:

- Implementing (automated) screening systems which screen customer and transaction information for matches with known PEPs;
- Incorporating thorough background searches into their CDD procedures, using tools such as:
- Manual internet search protocols;
- Public or private databases;
- Publicly accessible or subscription information aggregation services;
- Commercially available background investigation services.

9.6 Targeted Financial sanction

Where the customer is positive match to sanctions category for Proliferation of risk or Terrorism financing under UN Security Council or UAE National list of Individual and Entities, Memas is expected to freeze the funds or do not honor the transaction and within 24 hours of awareness of sanction individual/entity/beneficiary. It is prohibited to make any such funds/precious without the prior consent of the Executive Office of UAEIEC. In such instances, compliance officer shall immediately to notify through UAEIEC and Ministry of Economy through GoAML. In implementing the TFS, Memas must do the following;

Step-1 Subscribe:

Subscribe to the Executive Office Notification System to receive automated email notifications on any updates to the Sanctions Lists (Local Terrorist List or UN Consolidated List)

Step-2 Screen:

Memas must screen constantly their customers, potential customers, beneficial owners, and transactions to identify possible matches to the Local Terrorist List or UN Consolidated List (Refer www.uaeiec.gov.ae for the list).

Screening must be undertaken in the following circumstances:

1. Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
2. Prior to onboarding new customers/business relationships
3. Upon KYC reviews or changes to a customer's information.
4. Before processing any transaction.

Step-3 Apply Targeted Financial Sanctions:

1. Freezing of all funds: Freeze, without delay (within 24 hours) and without prior notice, all the funds:
 - Owned or controlled, wholly or jointly, directly, or indirectly, by an individual or legal entity designated by the UAE Cabinet or pursuant to a relevant UNSC Resolution.
 - Derived or generated from funds under item (a); or
 - Individuals or legal entities acting on behalf of or at the direction of an individual or legal entity designated by an individual or legal entity designated by the Local Terrorist or pursuant or the United Nations consolidated list.
2. Prohibition of making funds/supply of precious Metal or stones or equivalent: No individual or legal person in the UAE is permitted to provide services related to, whether in whole or in part, directly or indirectly, or for the benefit of any individual or legal entity listed in the Local Terrorist List or the UN Consolidated List pursuant to a relevant UNSC Resolution.

Step-4 Report:

Should report any freezing or suspension measures taken upon identifying confirmed or potential matches through the Go AML platform within five (5) days from taking such measures.

Refer Appendix 3 for additional obligations on Targeted Financial Sanctions.

9.7 Updation of KYC information

KYC information should be reviewed periodically, based on the risk categorization of the customer and supplier, with the Lowest Updating period being annually and Highest Risk Being Done every quarterly.

9.8 Use of Third party for CDD

Memas may use the third party in reliance on a third party of the entire or part of the CDD process as well as reliance on a third party when to introducing business. In selecting a third party, Memas should ensure that:

- The third party is regulated and supervised and adheres to the CDD measures towards Customers and record-keeping.
- The third party should also have adequate and effective control measure on Anti Money Laundering, Counter financing of Terrorism and Illegal organization and sanction measures.
- SLA is agreed with the third parties setting role and responsibilities of each party.
- Procedures for the certification by third parties of documents and other records pertaining to the CDD measures undertaken.
- Copies of the Identification and verification checks are made available as and when required.
- They reserve right to audit third party and their business relationship, customer and counterparty data, due diligence documentations.

Memas does not utilize foreign third party in carrying out CDD checks. However, when it chooses as such, it would ensure that the regulatory requirement and the data protection requirement of UAE are considered before offshoring such services.

10. TRAINING AND AWARENESS

Memas believes that one of the best tools to combat money laundering and terrorism financing is to create a culture of compliance and control among its staff. Training Program ensures that all the staff are mandatorily trained in AML and sanctions-related requirements at the time of joining and regularly on an on-going basis.

Staff will have access to the updated version of this policy and other policies and will be involved in the task of prevention, for which they will be duly informed and instructed. To ensure the continued adherence to AML/, CFT and Sanction policy, all staff of Memas are required to confirm and reconfirm their awareness of the contents of this Compliance Manual by signing the acknowledgement form annually, or more frequently, as required by the Compliance Officer.

All the staff will be provided with regular training periodically, its is mandatory that the staff be trained at least twice a Year.

11. RECORD RETENTION

At a minimum, all relevant records are retained:

- KYC Forms along with the identity and verification details;
- All documentation concerning a suspicious activity or suspicious transaction report concerning a client or applicant together with any response or follow up;
- High risk registers and rationale for acceptance and list of rejected cases;
- Any submissions of assessment to regulators or independent assurance outcomes;
- Records of AML/CFT training sessions attended by staff, officers and their affiliates, the dates, content and attendees

The following document retention periods shall be followed:

- All records of all transactions of covered clients, especially customer identification records, shall be maintained and safely stored in an easily accessible place for Five (5) years from the dates of transactions.
- With respect to closed relationships, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least Five (5) years from the dates when they were closed.
- If the records relate to ongoing investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed.
- The transaction may be store in the electronic format provided that such may be pursuant to the UAE Rules of the Court and E-Commerce Law. Memas ensure that adequate backup of the storage media is held either in cloud-based environment or at an off-site location within UAE.

13. NON-COMPLIANCE

- Any breach of this policy will be referred to the Compliance Officer who will review the breach and determine adequate consequences, which can include disciplinary procedures under HR procedures.
- Any violation or breach be subject to disciplinary proceedings in accordance with UAE Labor Law, the AML Regulations, and any other applicable UAE Laws.
- If employees are unsure or not clear of anything in this policy, they should seek clarification or advice from Compliance Officer.

14. REVIEW

The AML, CFT & Sanction policy shall be periodically reviewed and at least annually for accuracy and appropriateness.

APPENDIX 1:

RED FLAGS/POTENTIAL SUSPICIOUS ACTIVITY LIST

The Business Relationship, Counterparty, or Customer:

- Suddenly cancels the transaction when asked for identification or information.
 - Is reluctant or refuses to provide personal information, or the Memas has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
- Their business activities and corporate history;
 - The identity of the beneficial owner;
 - Their source of wealth/funds;
 - Why they are conducting their activities in a certain manner;
 - Who they are transacting with;
 - The nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
 - Is a designated person or organization (i.e. is on a Sanctions List).
 - Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
 - Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
 - Actively avoids personal contact without sufficient justification.
 - Is a politically exposed person, or has familial or professional associations with a person who is politically exposed.
 - Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for doing business with Memas .
 - Is located in a significant geographic distance away from the Memas , with no logical rationale.
 - Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
 - Makes unusual requests (including those related to secrecy).
 - Is prepared to pay substantially higher fees than usual, without legitimate reason.
 - Appears very concerned about, or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
 - Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
 - Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
 - Requests services that could improperly disguise the nature of the precious Metal and Stones or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.

- Claims to be a legitimate DPMS but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others).
- Is registered under a name that does not indicate that activity of the company is related to precious Metal and stones, or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorized the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of the unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for shortcuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Requests payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or instalment arrangements, or payment in several different forms), or which involve third parties.
- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be affected exclusively or mainly through the use of cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

The Transaction-Based Red Flags:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of precious Metal and stones (especially diamonds and gold) or Jewellery for cash in small incremental amounts.
- Involves the barter or exchange of precious Metal and stone (especially diamonds and gold) or Jewellery for other high-end Jewellery.
- Appears structured so as to avoid the cash reporting threshold.
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the counterparty or customer.
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves precious Metal and stones with characteristics that are unusual or do not conform to market standards.
- Involves the unexplained use of powers-of-attorney or similar arrangements to transact business on behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other authorized representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries, when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.

- Involves circumstances in which the parties:
- Do not show particular interest in the details of the transaction.
- Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
- Insist on an unusually quick completion, without a reasonable explanation.
- Takes place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licenses, or other official requirements.
- Involves any attempt by a physical person or the 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, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under- shipments (e.g. false entries on bills of lading); or multiple trading of the same goods and services).

Means of Payment

- Involves cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or similar instruments), negotiable bearer instruments, or virtual currencies, which do not state the true payer, especially where the amount of such instruments is significant in relation to the total value of the transaction, or where the payment instrument is used in a non-standard manner.
- Involves unusual deposits (e.g. use of cash or negotiable instruments, such as traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below the reporting threshold limit) to pay for precious Metals and stones. The negotiable instruments may be sequentially numbered or purchased at multiple locations, and may frequently lack payee information.
- Is divided into smaller parts or instalments with short intervals between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.
- Cannot be reasonably identified with a legitimate source of funds.

APPENDIX 2 – GOAML

ABOUT GOAML SYSTEM

It is an internationally approved electronic system to collect and analyze financial and non- financial information to confront money laundering and combat the financing of terrorism. It aims to oblige finance establishment and DNFBPs to register in their systems and report for Suspicious Activity Reports, Suspicious and Unusual Transaction reports to the FIU. It thereafter enables the Financial Intelligence Unit (FIU) in the United Arab Emirates with better monitor trends during analyzing reports of suspicious activities and transactions to reduce potential threats at more efficient rate and potency.

Memas under the provision of the regulatory requirements, circulars is required to register their compliance officer to the Go AML system for reporting or raising any SARs/STRs/Unusual transactions.

To know more about the system and how to register, please click on the following link:

<https://www.moec.gov.ae/en/registering-companies-in-goaml>

APPENDIX 3 – TFS ADDITIONAL OBLIGATIONS

Implement the freezing cancellation decision	Without delay, pursuant to Related UN Security Council Resolutions or decisions of the Cabinet regarding issuance of Local Terrorist List, and notify the Supervisory Authority and the Executive Office.
Immediately notify	<p>Notify within five business days, the relevant Supervisory Authority and the Executive Office in the following cases and include the following information:</p> <ol style="list-style-type: none"> 1. Identification of targeted funds - the actions that have been taken as per requirements of related UNSC Resolutions or decisions of the Cabinet regarding issuance of Local Lists, including concerning attempted transactions. 2. Detection of any match with listed individuals or legal entities - details of its data and the actions that have been taken as per requirements of related UNSC Resolutions or decisions of the Cabinet regarding issuance of Local Terrorist Lists, including concerning attempted transactions. 3. If it was found that one of its previous customers or any occasional customer it dealt with, is listed on the Sanctions List or the Local Lists. 4. If there is any indication that one of its customers or former customers, or a person it has business dealings with, is a individual listed on the UN Sanctions List or the Local List or has a direct or indirect relationship with a Listed individual. 5. Similarity of names (notify even if no action has been taken / inability to remove such similarity through available or accessible information).
Implement internal controls and procedures	Set and effectively implement internal controls and procedures to ensure compliance with the obligations arising from the Cabinet Resolution No. 74 of 2020.
Implement policies and procedures	Set and implement policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action shall be implemented as per provisions of the Cabinet Resolution No. 74 of 2020.
Cooperate	Cooperate with the Supervisory Authority and the Executive Office in verifying accuracy of presented data

APPENDIX 4- Enhanced Due Diligence Format

Enhanced Due Diligence Review Template

Customer Onboarding Review	
Company Details	
Company Name	
TL Number	
Date of Incorporation	
Date of Expiry	
No Of years in Business	
Country of Incorporation	
MOA/AOA	
Nature of Business	
TRN Number Identified	
Value of Expected Transaction	
Source of Funds of Company	
Method of Payment	
UBO Identified and verified	
Website Details	
Screening Status	
PEP Association	
Share Holder Details	
Share Holder 1	
Name of Shareholder	
KYC of Shareholder	
Nationality SH	
Residency Status / Country	
Share % in Company	
Screening Status	
RESPONSIBLE SUPPLY CHAIN PROGRAME REVIEW	

Conformance to OECD Rules	
Origin of Gold Declared	
Responsible Supply Chain Policy	
Logistics of Precious Metals	
Precious Metal Trading Agreement	
Anti-Bribery Policy	
Type of Gold Declared	
Risk Review Screening	
Risk Review Screening Company	
PEP Screening	
Sanction Screening	
Adverse Media Screening	
AML Programme Review	
Supply Chain Policy	
OECD Country Risk Rating	
Know Your Country Review	
Risk Review Screening Shareholders	
PEP Screening	
Sanction Screening	
Adverse Media Screening	
AML Review	
World Check Screening	
OECD Country Risk Rating	
Know Your Country Review	
Documentation Status	
PEP Declaration	
AML Policy of Company	
Sanction Declaration	
Conformance to Non-Conflict	
Account Opening Form	
UBO KYC	

Company KYC	
Additional Miners and Exporters Documentation (Only for International Suppliers)	
Mine License Number	
Gold Export License Copy	
Mining Policy	
Exploration License/Permit	
Origin of Gold Declaration	
Feed Back of Review	
List of Missing Documents	
Findings and Recommendation of Compliance Officer	
COMPLIANCE HEAD REMARKS	

Details	Names	Signature
Prepared by		
Approved by		

APPENDIX 5-

Standard Due Diligence Format and Risk Grading

Name of Entity:		
Length of Business	Risk Factor	Risk Grade
	Up to 1 year	Medium Risk
	1 year and above	Low Risk
Date of Expiry	Risk Factor	Risk Grade
	Unwilling to give Documents	High Risk
	Expired Documents	Medium Risk
Nature of Business Matching with Profile	Risk Factor	Risk Grade
	No	High Risk
	Yes	Low Risk
Country of Registration	<i>To be Identified from the Account Opening Form</i>	
Risk Rating of the Country of Incorporation	<i>Based on the Know Your Country Risk Rating and FATF Rating – Classification would be based on Low Risk, Medium Risk and High Risk – Risk Grading methodologies are explained in the AML Policy.</i> .https://www.knowyourcountry.com/methodologies-sources	
Type of Company Establishment	<i>To be identified via Trade License</i>	
	Risk Factor	Risk Grade
	LLC- UAE	Low Risk
	FZE- UAE	Low Risk
Licensing Authority	<i>To be Identified from the Account Opening Form</i>	
	<i>To be identified via Trade License and MOA</i>	
	Risk Factor	Risk Grade
Ownership Structure Break Up how many Shareholders less than 25% with KYC documents	With KYC Document	Low Risk
	Majority of Shareholder > 25% without KYC	Medium Risk
	Shareholders Without documents	High Risk
TRN Number Identified	Risk Factor	Risk Grade
	No	High Risk
	Yes	Low Risk
Shareholders Identified via Proper KYC documents	Risk Factor	Risk Grade
	No	High Risk
	Yes	Low Risk
Shareholders nationality Risk Factor	<i>Based on the Know Your Country Risk Rating and FATF Rating – Classification would be based on Low Risk, Medium Risk and High Risk – Risk Grading methodologies are explained in the AML Policy</i> https://www.knowyourcountry.com/methodologies-sources	

Source of Funds Identified	<i>To be Identified from Account Opening Form and Audited Financial Statement / Bank Statement</i>
PEP Factor Identified for Shareholders	<i>To be Identified from Account Opening Form and Conducting world Check</i>
Declaration of Not Sourcing from High-Risk Country	<i>To be Identified from Account Opening Form and Document Collection</i>
Implementation of Go AML UAE	<i>To be Identified from Account Opening Form</i>
Implementation of AML Policy	<i>To be Identified from Account Opening Form and Collecting of Policy</i>
Implementation of UAE Cabinet issued Resolution (74) of 2020?	<i>To be Identified from Account Opening Form</i>
Responsible for Sourcing of Precious Metal	<i>To be Identified from the Account Opening Form and Collection of Policy</i>
Complete Account Opening Forms	<i>To be Identified from the Account Opening Form</i>
Review Final Rating	