PROMISE GOLD REFINERY (FZC)

POLICY MANUAL FOR THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCINGOF TERRORISM

PGR-AML-2023-REV001

2023

250 M2 Warehouse T5-073 Sharjah - U.A.E

POLICY STATEMENT

Promise Gold Refinery FZC, as a business entity and trade license holder conduct following business in the UAE recognized as Dealers in precious metals & Stones also known to have its activities categorized under Designated Non-Financial Businesses & Profession "DNFBP's" by its supervisory authorities.

Promise Gold Refinery FZC offers commercial services to the public which include; the refining of precious metals, sales and trading of precious metals, purchase and refining of recycled/scrap metal, the production of finished products.

The management understands the importance of application of the standards and guidelines issued by Ministry of Economy and the supplementary guidance for industry best practices while doing the transactions and conducting businesses in the UAE.

The management of Promise Gold Refinery FZC believes that the best way to fulfill this commitment is to establish effective AML/CFT policies, procedures, internal policies and processes that are conducive to:

- Carrying out the activities and services provided in accordance with strict ethical standards and current laws and regulations.
- The implementation of codes of conduct and monitoring and reporting systems to prevent that the company is used for money laundering and terrorism financing.
- Ensuring that all the employees of Promise Gold Refinery FZC observe this policy manual and performs action to the adherence of the processes mentioned in it.

This Policy Manual is:

Reviewed and recommended by		**Approved by**	
Name	Mohammad Trahum Nawaz Shamsi	**Name**	Vipin Raj Selvaraj
Designation	**Compliance Officer/ MLRO**	**Designation**	Managing Director
Signature		**Signature**	
Date	**01.06.2023**	**Date**	**01.06.2023**

TABLE OF CONTENT

2. BASIS OF POLICY FORMULATION AND REFERENCES

This policy document is based on the guidelines issued by the following regulatory authorities and trade bodies, the document is in adherence with all applicable UAE Laws and Regulations as mentioned herein, the activities of Promise Gold Refinery FZC ultimately is dependent on local Banks & Licensed Financial Institutions (LFI's) for conducting and completing its financial transactions related to the business activities conducted., it's imperative for the company to abide by all laws and regulations related to AML/CFT which directly or due to its relationships with LFI's may have an impact on its trading activities. The below mentioned laws and regulations have been taken into consideration to enhance Promise Gold Refinery FZC overall AML/CFT Compliance Regime.

- Decree Federal Law No. (20) of 2018 on AML & CFT and Illegal Organizations
- Decree Federal Law No. (26) of 2021 amending certain provisions of Federal Decree Law No. 20 for2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.
- Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. (20) of 2018.
- Cabinet Decision No. (20) of 2019 regarding terrorism lists regulation and implementation of UNSCRs on the suppression and combating of terrorism, terrorist financing and proliferation of WMDand related resolutions.
- Cabinet Decision No. (74) of 2020 regarding implementation of UNSCRs
- CBUAE Notice No. 74/2019 (19/6/2019) - Procedures on AML/CFT and illegal organizations.
- CBUAE Notice No. 79/2019 (27/6/2019) - Guidelines on AML/CFT and illegal organizations.
- CBUAE Notice No. 103/2020 (24/3/2020) - Regarding UN and Local Lists.
- Federal Law No. (7) of 2014 regarding terrorism offences.
- GoAML Notice - High Risk Country Transaction & Activity Report - 13/04/2021(Part of RBA)
- Notice No. 3090/2021 - Updated Guidelines on AML / CFT & Illegal Organizations
- Notice No. 3236/2021 - Guidance for LFI's providing services to the Real Estate and Precious Metals& Stones sector.
- Notice No. 3895/2021 - Implementation of UN Security Council (UNSC) and UAE Cabinet Resolutionsregarding UNSC and Local Lists
- Notice No. 2893/2021 - Guidance on TFS & Typologies on the circumvention of Targeted Sanctions against Terrorism & Proliferation of Weapons of Mass Destruction
- Notice No. 3556/2021 - Guidelines on AML & Countering Terrorist Financing
- Notice No. 3551/2021 - Guidance for LFI's - Implementation of Targeted Financial Sanctions
- Notice No. 3091/2021 - Guidance for LFI's on Suspicious Transaction Reporting
- Notice No. 4593/2021 - Guidance for LFI's Providing Services to Cash-Intensive Businesses
- Notice No. 4415.2021 - Typologies on AML & CFT in the Financial Sector
- Notice No. 4368.2021 - Guidance for LFI's on Transaction Monitoring & Sanctions Screening
- Notice No. 4711/2021 - AML/CFT & Illegal Organizations Controlled & Dual use Goods for FIs
- Guidance on Targeted Financial Sanction for FIs, Company and VASPs issued by the EOCN (Executive Office for Control & Non-Proliferation)

All other relevant laws/regulations and Typology Reports issued by UAE on AML/CFT andinternational initiatives and best practices therein.

2.1 THE MINISTRY OF ECONOMY

The Ministry of Economy is fully committed to countering money laundering, combating, detecting, and deterring terrorist financing in accordance with legislation, as the relevant authorities in the UAE have established an institutional system of supervision, control and gathering information on all practices that may lead to and respond to financial crimes, including money laundering and terrorist financing. The authorities are aware that the national framework and coordination to address money laundering and combat terrorist financing must continue to be strengthened and developed to improve its effectiveness.

As a reporting entity for Designated Non-Financial Businesses and Professions (DNFPB) expects:

- Strict compliance with applicable Anti-Money Laundering and Terrorism Financing Laws - Decree20 of the Federal Law 2018 on countering money laundering offences, combating terrorist financing and financing illegal organizations and
- As well as with the recommendations and circulars issued on this subject - Regulations 10 of 2019 for a decree of federal law No. 20 of 2018 on countering money laundering crimes, combating terrorist financing, and financing illegal organizations
- Cabinet Decision No. (20) of 2019 Terrorism List Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and proliferation of Weapons of Mass Destruction, and Related Resolutions.
- Cabinet Resolution No. (16) of 2021 on the Consolidated List of Offences and Administrative Fines.
- Cabinet Resolution No. (53) for 2021 on administrative sanctions resulting from violators of the provisions of The Council of Ministers Resolution No. (58) for 2020.
- Cabinet Resolution No. (58) for 2020 on regulating the actions of the real beneficiary
- Cabinet Resolution No. (74) of 2020 on the system of lists of terrorism and the implementation of Security Council resolutions on the prevention, suppression and financing of terrorism, cessation of arms proliferation and financing and relevant resolutions.
- 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 Organization's (the "AML-CFT Decision").

Website: www.economy.gov.ae

2.2 THE CENTRAL BANK OF UAE:

The Central Bank of the United Arab Emirates is the state institution responsible for managing the currency, monetary policy, and banking regulation in the United Arab Emirates (UAE).

The Central Bank of the UAE has powers to issue and manage the currency.

- to ensure the stability of the currency.
- to manage the UAE's credit policy.
- to develop and oversee the banking system in the UAE.
- to act as the Government's banker.
- to provide monetary and financial support to the Government.
- to manage the UAE's gold and currency reserves.
- to act as the lender of last resort to banks operating in the UAE; and
- to represent the UAE in international institutions such as the International Monetary Fund, theWorld Bank, and the Arab Monetary Fund.

The Central Bank of UAE has the following functions: -

- Branches
- Banking Supervision and Examination Department
- Banking Operations Department
- Research and Statistics Department
- Administration Affairs Department
- Financial Control Department
- Treasury Department
- Internal Audit Department

UAE LAWS ON AML/CFT, FRAUDS, ANTI-BRIBERY AND CORRUPTIONS

- CBUAE regulation 24/2000 and covers the area of corruption laws.
- Federal Law 4/2002 regarding the Criminalization of Money Laundering.
- Federal Law 9/2014 amending certain provisions of Federal Law 4/2002 concerning theCombating of Money Laundering Crimes.
- Dubai Law 4/2016 on Financial Crimes.
- Cabinet Resolution 38/2014, Executive Resolution of Federal Law 7/2014, Combating Terrorism Crimes regulations regarding declarations by travelers entering or leaving the United Arab Emirates carrying cash and monetary or financialbearer instruments (issued in 2011).
- Federal Decree Law No 20 of 2018 issued by Ministry of Finance.
- The Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business("the Standards") Version 1.10 (February 2018)
- National Risk Assessment, issued by National Committee for combating ML/TF (NAMLCFTC)(June 2019)
- Cabinet decision No (10) 2019, issued by Ministry of Finance, (June 2019)

2.3. UNITED NATIONS:

United Nations is an intergovernmental organization to promote international co-operation. It was established on 24th of October 1945. At its founding, United Nations had 51-member states. Currently United Nations has 153 members. The headquarters of the United Nations is in Manhattan, New York, USA. The organization is financed by assessed and voluntary contributions from its member states. Its objectives include maintaining international peace and security, promoting human rights, fostering social and economic development, protecting the environment, and providing humanitarian aid in cases of famine, natural disaster, and armed conflict.

The UN has six principal organs:

- The General Assembly (the main deliberative assembly).
- The Security Council (for deciding certain resolutions for peace and security);
- The Economic and Social Council (ECOSOC) (for promoting international economic and social co-operation and development);
- The Secretariat (for providing studies, information, and facilities needed by the UN);
- International Court of Justice (the primary judicial organ); and
- The United Nations Trusteeship Council (inactive since 1994).

UN System agencies include the World Bank Group, the World Health Organization, the World Food Program, UNESCO, and UNICEF.

United Nations Security Council: The Security Council is charged with maintaining and security among countries. While other organs of the United Nations can only make "recommendations" to member states, the Security Council has the power to make binding decisions that member states have agreed to carry out, under the terms of Charter Article 25. The decisions of the Council are known as United Nations Security Council resolutions.

The Security Council is made up of fifteen-member states, consisting of five permanent members—China, France, Russia, the United Kingdom, and the United States—and ten non- permanent members. The UN Charter is a multilateral treaty. It is the constitutional document that distributes powers and functions among the various UN organs. It authorizes the Security Council to act on behalf of the members, and to make decisions and recommendations. Resolutions by the Security Council are legally binding if they are made under Chapter VII of the Charter.

Websites:

- http://www.un.org
- http://unscr.com

1.4. Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering (FATF) was established in 1989 at G7 Summit in Paris to combat the growing problem of money laundering. The task force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering.

At the time of its creation, the organization had 16 original members. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In its first year, the FATF issued a report containing forty recommendations to fight money laundering more effectively. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering. In 2001 the purpose expanded to act on terrorism financing. In February 2012, the FATF codified its recommendations and Interpretive Notes into one document and included new rules on weapons of mass destruction, corruption and wire transfers.

FATF monitors countries' progress in implementing the FATF Recommendations by 'peer reviews' ('mutual evaluations') of member countries.

Website: http://www.fatf-gafi.org/

3. INTRODUCTION:

Promise Gold Refinery FZC, hereafter may be referred as "Promise Gold Refinery, Company, Organization, Entity, We, us",

Promise Gold Refinery FZC maintains high standards of professional, social, business ethics and relationship with regulators, customers, peers, developers, and other internal and external stakeholders.

Promise Gold Refinery FZC understands that the business activity of the company is highly Vulnerable to Money Laundering and Terrorist Financing Risks due to the fact that:

- Precious Metal and Stones (PMS) represent high intrinsic value in a relatively compact form, tend to maintain (or even increase) value over time, and can be easily transported physically in many forms.
- Precious Metal and Stones can be used both as means to generate criminal proceeds (i.e., through various predicate offences), as well as vehicles to launder them.
- Precious Metal and Stones can be used for illicit purposes, including ML/TF, in a variety of ways, either directly (through physical exchange, as a form of currency) or indirectly (through exchange of value via various formal and informal financial systems, as well as via international trade and the financial products and services related to it)

There are large, well-established, decentralized, and often cash-based markets for certain types of precious metals and stones (particularly for gold and diamonds, but for other PMS as well), often allowing them to be traded or exchanged with relative anonymity.

In its relentless efforts to exercise caution in all its transactions, organization have planned to implement policies and procedures and provide suitable trainings to its staff for the awareness and implementation of guidelines as issued by the Ministry of Economy on AML/CFT.

This internal policy is based on the guidelines issued by the Ministry of Economy for DNFPBs and Supplemental Guidance for Dealers in Precious Metals and Stones in the UAE, and other international recommendations and practices by FATF.

3.1. GOVERNANCE FRAMEWORK:

3.2. Roles and Responsibilities:

3.2.1. Management Roles and Responsibilities: Owner

3.2.1.1. Minimum requirements:

Owner of Promise Gold Refinery FZC must undertake and govern the compliance activities and functions in Promise Gold Refinery FZC.

Following Functions Shall be undertaken by the Owner:

- Undertake a risk assessment which identifies the vulnerability of the company to be used to launder money or finance terrorists.
- Based on the risk assessment, implement a risk management framework to ensure that the company is not used to launder money or finance terrorists.
- Ensure that the risk management framework is developed, and sufficient resources being devoted to dealing with higher-risk customers and transactions.
- Ensure that the company has appropriate compliance management arrangements, including the appointment of a compliance officer at management level; and
- Devote sufficient resources to deal with money laundering and terrorist financing, including ensuring that the compliance function is adequately resourced, and that staff receive appropriate and adequate training.

3.2.1.2. Actions required. Owner Must:

- Carry out a risk assessment, which should be reviewed and updated on a regular basis, identifying where the business is vulnerable to money laundering and terrorist financing.
- Based on the risk assessment, develop internal policies, procedures, and controls to combat money laundering and the financing of terrorism.
- Ensure staff effectively implement the internal policies, procedures, and controls and receive appropriate training; and
- Monitor the implementation of the company policies, procedures, and controls and make improvements where required on the basis of changes to the company`s money laundering and terrorist financing risk assessment or as recommended by the regulatory authority and/or the financial intelligence unit.

3.2.1.3. Responsibilities

- Owner is responsible for the effective implementation of a risk framework of money laundering and terrorist financing risk.
- The management of risk needs to be reviewed and updated from time to time to reflect changes in the company`s strategy or other factors such as changes to the law.
- Policies and procedures should consider risk factors relating to the customer, product and service, delivery channel, and geographic location of the customer.
- Where higher risks are identified, based on the Company`s risk assessment, the staff must take extra measures and senior management should ensure that the staff fully understand and implement the requirements of the policies and procedures.

3.2.2. Management Roles and Responsibilities – Compliance Officer

The Anti-Money Laundering Officer is responsible for the following actions:

1. **Regulatory Compliance**

- Monitoring Regulatory Changes: Stay updated on laws and regulations related to precious metals trading, Anti-Money laundering (AML), know your customer (KYC), and other relevant standards.
- Policy Development: Develop, implement, and maintain compliance policies and procedures to ensure the firm meets all legal and regulatory requirements.
- Regulatory Reporting: Ensure timely and accurate submission of reports to regulatory bodies.

2. Risk Management

- Risk Assessment: Conduct regular risk assessments to identify and mitigate potential compliance risks, including market, operational, and reputational risks.
- Internal Audits: Oversee or coordinate internal audits to verify compliance with established policies and procedures.
- Incident Management: Investigate and manage compliance incidents or breaches, ensuring appropriate corrective actions are taken.

3. Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF)

- KYC Processes: Ensure that the firm follows robust KYC processes to verify the identity of clients and counterparties.
- Transaction Monitoring: Implement and monitor systems for detecting and reporting suspicious activities, including unusual trading patterns or transactions.
- Training and Awareness: Provide regular AML and CTF training to employees to ensure they understand their responsibilities and can identify potential red flags.
- Reporting FIU portal for GO AML and SAR /STR

4. Ethical Standards and Corporate Governance

- Code of Conduct: Enforce the firm's code of conduct and ensure that all employees adhere to high ethical standards.
- Conflicts of Interest: Monitor and manage potential conflicts of interest within the firm, ensuring that they are disclosed and handled appropriately.
- Whistleblowing Mechanism: Establish and manage a whistleblowing mechanism that allows employees to report unethical behavior or compliance concerns anonymously.

5. Training and Education

- Employee Training: Organize and conduct regular training sessions for employees on compliance-related topics, including regulatory changes, ethical practices, and internal policies.
- Ongoing Education: Keep the firm informed of new regulations, best practices, and industry trends through continuous education programs.

6. Collaboration and Communication

- Internal Communication: Act as a liaison between the compliance department and other departments, ensuring clear communication of compliance requirements and updates.
- External Communication: Maintain relationships with regulators, auditors, and other external stakeholders, ensuring transparent and open communication.

7. Documentation and Record Keeping

- Records Management: Maintain comprehensive records of all compliance-related activities, including audits, training sessions, and incident reports.
- Documentation of Policies: Ensure that all compliance policies and procedures are well-documented and easily accessible to relevant stakeholders.

8. Advisory Role

- Guidance to Management: Provide advice to senior management on compliance issues, helping them make informed decisions that align with regulatory requirements.
- Strategic Input: Contribute to the firm's strategic planning by ensuring that compliance considerations are integrated into business decisions.

9. Continuous Improvement

- Compliance Program Review: Regularly review and update the firm's compliance program to reflect changes in the regulatory environment and business operations.
- Benchmarking: Compare the firm's compliance practices against industry standards and competitors, striving for best-in-class performance.

4. AML/CFT GUIDELINE AND PROCEDURES:

4.1. Risk based Approach (RBA).

A risk-based approach (RBA) is central to the effective implementation of the AML/CFT legislation. It means that Promise Gold Refinery FZC must identify, assess, and understand the ML/TF risks to which they are exposed, and implement the most appropriate mitigation measures. An RBA requires Promise Gold Refinery FZC to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good AML/CFT compliance program and will enable the company to focus their resources where the risks are higher depending upon nature, size and complexity of the bullion business.

Promise Gold Refinery FZC as dealers in precious metals and stones should carefully consider the following factors while conducting any business relationship (Including Supplier, Customers and third-party vendors providing goods/services) with a natural person/Individual, legal entity, or a corporate customer such as

Customer Risk: Whether the counterparty or customer is a physical person, a legal person, or a legal arrangement, if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a Political Exposed Person (PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate.

- ✓ **Type of customers:** The risks related to retail customers in combination with their product/service needs may be different from those related to high net worth or corporate customers and their respective product/service needs. Likewise, the risks associated with resident customers may be different from those associated with non-resident customers.
- ✓ **Customer base:** As Promise Gold Refinery FZC will be dealing with a customer base that is engaged in the business of precious metals and hence the customer risk classification will be dome accordingly.

- ✓ **Maturity of relationships:** The company has to carefully consider the length of the business relationship and the frequency of transaction while determining risk factors.

Some of these customer risk factors are also relevant when determining the customer risk classification of an individual customer and the type and extent of customer due diligence to be performed.

Geographic Risk: Country of origin of the product, particularly in relation to whether the country is a known production or trading hub for the type of precious Metals and Stone; has adequate regulations and controls (for example, is a participant in the Kimberley Process Certification Scheme (KPCS) for rough diamonds); is a High-Risk Country (e.g., is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist Organization's).

Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country).

Regulatory/supervisory framework. Countries with stronger AML/CFT controls present a different level of risk than countries with weaker regulatory and supervisory frameworks, for instance countries identified by the FATF as jurisdictions with weak AML/CFT measures.

International Sanctions. Company should consider whether the countries or jurisdictions they deal with are the subject of international sanctions, such as targeted financial sanctions (TFS), UAE, OFAC, UN and EU restrictive measures, that could impact their ML/FT risk exposure and mitigation requirements.

Reputation. Company should consider whether the countries or jurisdictions they deal with are associated with higher or lower levels of ML/FT, corruption, and (lack of) transparency (particularly as regards financial and fiscal reporting, criminal and legal matters, and Beneficial Ownership, but also including such factors as freedom of information and the press).

Combination with customers' inherent risk factors. Company should consider the countries risk in combination with customers risks, including principal residential or operating locations of customers.

Product-, Service-, Transaction-Related Risk: When assessing the inherent ML/FT risks associated with product, service, and transaction types, a DNFBP should take stock of its lines of business, products and services that are more vulnerable to ML/FT abuse. Company should assess the inherent ML/FT risks of abuse of the products and services by their customers considering a number of factors such as their ease for holding and transferring value or their complexity and transparency. Some of the risk factors that Company should consider, among others, are:

- ✓ **Typology:** Company should consider whether the product, service, or transaction type is associated with any established ML/FT typologies.

- ✓ **Complexity:** Products, services, or transaction types that favour complexity, especially when that complexity is excessive or unnecessary, can often be exploited for the purpose of money laundering and/or the financing of terrorism or illegal Organizations. Company should consider the conceptual, operational, legal, technological and other complexities of the product, service, or transaction type. Those with higher complexity or greater dependencies on the interactions between multiple systems and/or market participants may expose Company to different types and levels of ML/FT risk than those with lower complexity or with fewer dependencies on multiple systems and/or market participants.

- ✓ **Transparency and transferability:** Situations that favour anonymity can often be exploited for the purpose of ML/FT. Company should consider the level of transparency and transferability of ownership or control of products, services, or transaction types, particularly in respect of the ability to monitor the identities and the roles/responsibilities of all parties involved at each stage. Special attention should be given to products, services, or transaction types in which funds can be pooled or co-mingled, or in which multiple or anonymous parties can have authority over the disposition of funds, or for which the transferability of Beneficial Ownership or control can be accomplished with relative ease and/or with limited disclosure of information.

- ✓ **Size/value.**: Products, services, or transaction types with different size or value parameters or limits may pose different levels of ML/FT risk.

Channel Risk: Channel by which the counterparty/customer is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy).When evaluating delivery channel-related risk, Company should pay particular attention to those channels, whether related to customer acquisition and/or relationship management, or to product or service delivery, which have the potential to favor anonymity. Among others, these may include non-face-to-face channels (especially in cases where there are no safeguards in place such as electronic identification means), such as internet-, phone-, or other remote-access services or technologies; the use of third-party business introducers, intermediaries, agents or distributors; and the use of third-party payment, or other transaction intermediaries.

Other Risk Factors: Given the ever-evolving nature of ML/FT risks, new risks are constantly emerging, while existing ones may change in their relative importance due to legal or regulatory developments, changes in the marketplace, or as a result of new or disruptive products or technologies. For this reason, no list of risks can ever be considered as exhaustive.

Nevertheless, additional factors that may present specific risks are, e.g., the introduction of new products or services, new technologies or delivery processes or the establishment of new branches and subsidiaries locally and abroad.

All the above factors to be assessed while onboarding a customer as part of Risk Assessment factors.

4.2 Customer Due Diligence: (Customers/Supplier & Support Agency)

Procedure to onboard a customer. (Refer Annexure).

Following documents to be collected as part of Due Diligence Process:

- KYC Registration Form (Refer Annexure)
- National ID of an Individual and all Partner/Shareholders/Owners/UBO.
- Passport copy of an Individual and all Partner/Shareholders/Owners/UBO.
- Business Registration License Copy with Online Verification QR code or in absence attested by UAE Embassy from the respective country.
- Permanent Residential Address of an Individual and all Partner/Shareholders/Owners/UBO.
- Tax Certificate if any in case of a Legal Entity.
- Memorandum of Association / Articles of Association in case of legal entity.
- Annual Audited Financial Statement to understand business volumes and turnover of the company if the volumes are more than the usual transactions.
-

Promise Gold Refinery FZC is registered for the updates at https://www.uaeiec.gov.ae / for Local Terrorist List and UN Consolidated list.

As a DNFBP (DPMS), Promise Gold Refinery FZC owes a responsibility towards the screening names and addresses against UN Consolidated Sanctions and Local list which is compiled and updated on a regular basis and kept in records for the purposes of identifying designated and prohibited individuals and entities, PEPs and other high-risk entities who may pose a threat to the international community at large. Name screening should be done for all the customers of the organization and for all the onboarding of the relations and related parties.

There are four main obligations on all persons, natural or legal in the UAE to implement Targeted Financial Sanctions (TFS)

4.2.1. Requirements:

- Promise Gold Refinery FZC should follow the strict adherence to the name screening on each transaction and ensure that no transaction is done with the customer's name that appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or any blacklist provided by the UAE Regulatory Authorities.
- Promise Gold Refinery FZC ensures that the Name Screening is done on a regular and transactional basis.
- Promise Gold Refinery FZC has an automatic name screening system which is integrated with the core system for a real time basis, scans, and filters names of each customer and beneficiary against the sanctioned list.
- In the event that there is a possible match of a customer name with that of the blacklist, there is a provision to put the transaction on hold.
- The details of the name match on the SDN list are checked against details of the customer and beneficiary.
- In the event of an exact match i.e., it is determined that the name is on the blacklist, the transaction is withheld and immediately reported to the Financial Intelligence Unit and the regulatory authority.
- Promise Gold Refinery FZC understand that the failure to report the same could result in fines, penalties, reputational and commercial loss.
- In the event the details of the customer do not match with the SDN list, the transaction and onboarding is released for further processing.
- The blacklists should be updated on a regular basis to avoid omission of names which may be recently added or deleted by the above-mentioned authorities.
- Promise Gold Refinery FZC maintains its internal watch list for addition and deletion of the persons with whom the company does not want to deal with according to the risk he/she may expose the company to.
- Any name screening that Identifies as PEP or on sanctioned list is escalated for the approval of the owner with the detailed EDD on the customer.
- The Logs related to the screening of the transactions should be kept for 5 years from the date of transaction for records.

4.3 SAR and STR Procedures

As a primary requirement of submitting Suspicious Transaction Reports (STR), Promise Gold Refinery FZC has obtained access to GoAML, the online STR reporting portal of the Central Bank. The Licensed Person may contact the FIU or the AML Department at Ministry of Economy for appropriate guidance to obtain access to the STR reporting portal.

All employees of the Promise Gold Refinery FZC are obliged personally to report, when there are reasonable grounds to suspect that the funds are proceeds from criminal activity or to be used for money laundering, terrorism or terrorist act or terrorist financing, to the compliance officer. The compliance officer will conduct proper investigations and update the highest authority and raise suitable STR/SAR's.

A single Suspicious Transaction Report (STR) can help stop the flow of illegal money and help prevent the repercussions of financial crime. Further, these reports are an essential contribution to the development of the financial intelligence resources that are used by country's law enforcement, revenue, and national security agencies. Thereby, we file STRs to ensure that the Promise Gold Refinery FZC is not used to aid the transfer of illegal money for money laundering and terrorism financing.

4.3.1. Procedures:

- All employees are required to report any potentially suspicious or unusual transactions.
- The reporting must be done with full facts of the case within reasonable time.
- It is company`s obligation to investigate the background and purpose of transactions deemed to be 'unusual' and to set forth our findings in writing, even in the event, it is not considered necessary to report the transactions to FIU as suspicious. As is the case of other documents these findings should also be maintained for inspection by the competent authorities for a period of at least five years.
- The Compliance Officer shall conduct in depth investigation and take an appropriate action before reporting such transactions to Financial Intelligence Unit.
- It is important to note that the "time factor" in reporting suspicious transactions remains crucial; if we are able to retrieve / submit the relevant information, it will help regulatory authority and Law enforcement authorities to effectively review and take effective measures to combat money laundering, terrorism financing or any other illegal activity.
- Attempted Transactions are obliged to report transactions through GoAML system, which appear as an attempt to launder money and / or finance a terrorist organization and / or a terrorist activity, Terrorism Financing.
- In case of doubt that a transaction might be meant for terrorism or terrorist organizations or for terrorism purposes, we should freeze the transaction / account and inform the financial intelligence unit in writing immediately.

All Employees should strictly comply with the following if a transaction created at your end / found in the system seems suspicious to you:

- Do not inform the customer of your suspicions about his/her transaction(s), and action being taken by you.
- Hold the transaction and report immediately to your Compliance Officer.
- Forward copy of Customer identity and transaction copy to Compliance Officer
- Hold or block the transaction and do not proceed.

Institutions which fail to report unusual and suspicious transactions shall be penalized in accordance with the prevailing laws and regulations, such incidents should be immediately reported to the authorities through the proper systems.

4.3.2 Tipping Off:

All suspicious transactions must be kept fully confidential, and no one should inform any person or customer that his/her transaction is being reported as a suspicious transaction to the FIU.

Non-compliance is a criminal offence, and the employee involved shall be terminated, immediately and additionally he/she is personally subject to a fine or imprisonment or both.

It is a criminal offence for an employee to tip off, tell or inform any person including customers that any of their transactions is being scrutinized for possible involvement in suspicious money laundering operations or terrorist financing.

4.4. Red Flags, Unusual, Suspicious Customer and Transactions Few key indicators of suspicious Customers and Transactions are:

4.4.1. 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 DPMS 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 are they 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 the DPMS.
- Is located a significant geographic distance away from the DPMS, 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) of the DPMS or its employees.
- 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 (for example, smelting and reshaping of gold into ordinary-looking items, or re-cutting and polishing precious stones) that could improperly disguise the nature of the PMS 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 PMS, 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 unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Request's 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.

4.4.2. Transactions:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of PMS (especially diamonds and gold) or jewelry for cash in small incremental amounts.
- Involves the barter or exchange of PMS (especially diamonds and gold) or jewelry for other high-end jewelry.
- 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 PMS 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).

4.4.3. The Payments:

- 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 traveler's cheques, cashier's cheques, and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PMS. 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 a short interval 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.

4.5. Know Your Employee

Know Your Employee policy should be conducted have the following stages.

a) Pre- Employment Stage
b) Course of employment
c) Employee Conduct

4.5.1 Pre – Employment Stage:

Due diligence in KYE starts at the recruitment stage, to know if the promising candidates are telling the truth. At the initial stage references should be checked, reference check can be done by the organizationor by outsourced agencies.

References of a prospective employee - You can verify if there is any criminal conviction; this can beachieved by getting.

- A police clearance certificate from the police station of the last known residences.
- The relieving letter from the previous employer is taken.
- The past employer can be asked to provide few details like; did they really work for that company stated on the CV? Employment credentials such as designation, role, compensation, conduct and reason for leaving will be ascertained.
- How was their conduct of the prospective employee?
- References provided by the prospective employee can be requested to provide information which the prospective employee has stated on the resume' or job application.
- The references given by the candidate shall be contacted & affirmed. (First degree relations should not be hired)
- In case the verification or background check services are provided by a vendor, Company must ensure the standards & procedures the organization applies while conducting the check. Are their standards comparable to yours? Are there procedures reviewed by an independent firm.
- Screening of Employee names against the sanctions list.

4.5.2 Course of Employment:

Even though the reference checks have been applied, it is advisable to have random checks to ensure that the employee maintains its responsibility to be a trustee of the organization. It is good management practice to monitor your employees' performance and understand what makes them stick, but this routine procedure can also unearth internal threats to your business.

4.5.3 Employee Conduct:

Signs which could raise a signal for verifying the employees conduct and behavior: -

- **Staff Behavior**: A change in the employee's lifestyle, especially when the spending etc. by anemployee sees a drastic change then what an employee at the same level could afford.
- **Credit cards/Loans:** the employees availing frequent loans and credit cards should pose a question for the employer. Too many approvals and NOCs provided to employees can not onlylead to defaults but can also cause the organization to be blacklisted for getting further benefits from banks etc.
- **Overzealous nature and relation with select customers;** There could be possibilities of Customers offering bribes and commissions to employees for conducting frauds, embezzlements and money laundering, Frequent checks, and controls on the activities of employees can help detect these activities at an early stage.
- **Timing:** Many a times employees employed in critical areas of operations and accounts havebeen caught for internal frauds etc. These employees have been reported to have long workinghours, coming early before the time to office and sitting till late in office.
- **Compromising on data & system integrity:** employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely for mitigating any risk offraud.

5. REGULATORY REPORTING

As a DNFBP and registered Authority Promise Gold Refinery FZC has obligation to report transactions in GoAML System for the following transactions:

5.1. Transactions with Individuals

- All Cash transactions with individuals equal or exceeding AED 55,000.00 needs to be reported in the GoAML System.
- Exceptions: (Not to Report) – Any Credit Card /Cheque or Bank Transfer transactions of any amount. Only if Suspicious then to be reported through STR Option in GoAML System.

5.2. Transaction with Legal Entities

- All Cash/ International Wire Transfers / Transfers through Exchange Houses or Remittance Companies equal or exceeding AED 55,000.00 need to be reported in the GoAML System.
- All Settlements in USD with following qualifications.
  - Both Entities having accounts in UAE and transfers done for USD payments.
  - USD Settlements done between two Free zones Within UAE, having different bank accounts, and settlements between Free zone and onshore companies registered in the UAE.

Exceptions: (Not to Report)

- AED Settlement where both the parties have accounts in same bank in the UAE.
- AED Settlement where both the parties have accounts in different banks in the UAE.
- USD Settlement where both the parties have accounts in same bank in the UAE.
- Trade between related parties Mainland to Free zone having same bank account transactions and vice versa.
- Barter transaction (Exchange of Gold)
- Intra Company Transactions
- Transaction not routed through the UAE Bank Account.

Funds Freeze Report (FFR) and Partial Name Match Report (PNMR) filing with GoAML

As per UAE AML Laws, reporting entities are required to file two new reports viz., Funds Freeze Report (FFR) and Partial Name Match Report (PNMR).

As stipulated in the Cabinet Decision (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," and as a part of the obligation for Targeted Financial Sanctions (TFS) reporting, reporting entities in UAE are supposed two submit two new reports in the GoAML portal.

Submission of Funds Freeze Report (FFR) and Partial Name Match Report (PNMR) with GoAML

1. **Funds Freeze Report (FFR)**
   Reporting entities are supposed to file Funds Freeze Report to report any freezing measure, prohibition to provide funds or services, and any attempted transactions related to 'confirmed matches.

2. **Partial Name Match Report (PNMR):**
   Reporting entities are supposed to submit Partial Name Match Report (PNMR) for any 'potential match.'

Further, the GoAML Registration portal now allows using the following Reasons for Reporting (RFRs):

- **TFS/PFS – Domestic List**
- **TFS/PFS – UNSCRs**

The Reporting entities are required to use the correct and most applicable Reasons for Reporting (RFRs) when submitting the TFS/PFS: Domestic List and TFS/PFS – UNSCRs via GoAML.

Further, Reporting Entities are expected to take all measures required as per cabinet decision (74) of 2020 in line with the procedures or guidance received from their supervisory authorities.

Reporting Entities should consult the published guidelines issued by their supervisory authorities and the Executive Office – IEC published guidelines, respectively, as updated from time to time in this regard.

A link to the Executive Office – IEC's website is found herein:

https://www.uaeiec.gov.ae/en-us/un-page

It is important that Promise Gold Refinery FZC also follow the guidelines provided in circular no. 1 of 2022: implementation of targeted financial sanctions on UNSCRS 1718 (2006) and 2231 (2015).

6. INDEPENDENT REVIEW:

A robust AML Compliance program shall be complete where a periodic review to assess the adequacythe policies & procedures, compliance officer's functions and other controls is performed.

The purpose of independent review is to review and test whether the policies, procedures & controlsare in line with the regulatory guidelines and to suggest changes and modifications in procedures to have more effective controls in the fight against money laundering and terrorism financing.

6.1 Guidelines:

Both internal & external audits play an important role in evaluating the procedures of Promise Gold Refinery FZC.

- **External Audit:** means testing of the internal procedures by an independent party i.e., performed by people not from within the company. The auditors must be sufficiently qualifiedto ensure that their findings and conclusions are reliable. It is advisable to conduct the independent testing by an external audit firm shall be on an annual basis.

- **Internal Audit:** these audits may be performed internally within an organization if there is aprovision of an internal audit department or could be outsourced to the efficient partners.

  - There should be a well-defined audit program & checklist.
  - The frequency of such audits may be once in 6 months.
  - The auditor should report directly to the Owner for its findings.

6.2 SCOPE:

- Examine the adequacy of CDD policies, procedures, and processes, and whether they complywith internal requirements.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations(products, services, customers, and geographic locations) on sample testing basis.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, trainingschedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AMLcompliance program if any.
- Reviewing policies, procedures, and processes for suspicious activity monitoring.
- Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.
- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluationof the research and referral of unusual transactions. Testing should include a review of policies,procedures, and processes for referring unusual or suspicious activity from all business linesto the personnel or department responsible for evaluating unusual activity.
- Assess the adequacy of recordkeeping.

7. TRAINING

The role of AML & CFT training in a dynamic business environment is to be a partner to the employees to help them achieve their objectives. This is achieved by developing the knowledge and skills of the employees. The success of learning, results from its integration with the business plan and the business culture. Hence the prime objectives for Training are:

- To enhance existing knowledge & skills of employees to enable them to successfully accomplish their duties and responsibilities.
- To upgrade the Product Knowledge of Front line / Operations & Sales Staff.
- To adhere to the guidelines of the regulatory authority on employee training.

7.1 Mandatory Teams for Trainings:

7.1.1 New employees – Induction Training

Newly joined employees need to undergo Induction program covering AML/CFT awareness and company`s procedural guide, within fifteen days from joining. This can be conducted internally by the qualified staff from AML/ Compliance Department or through external vendor having expertise in trainings and AML/CFT Knowledge.

7.1.2 Front Line Staff – Induction and Refreshers Training.

All sales staff acts as a first line of defense for AML/CFT program and needs to be trained on an annual basis. These training can be conducted internally by the qualified staff from AML/ Compliance Department or through an external vendor having expertise in trainings and AML/CFT Knowledge.

7.1.3 AML Compliance Department – Continuous Professional Development.

All the employees and members related to AML/Compliance Department shall undergo a Continuous professional development program every year. These trainings can be earned through:

- AML/CFT conferences or meetings or workshops whether inside or outside the UAE.
- Face to face training by external agencies whether inside or outside the UAE.
- Training by industry associations or regulatory bodies; and
- Web based training

7.1.4 Auditors:

Auditors acts as a third line of defense for AML Program, hence the need to undergo an Awareness and Assessment Training program to audit the operational and AML program implementation of the company. It is advised to conduct an external training program for auditor's minimum once in a year.

7.1.5 Senior Management – AML Awareness Program.

Senior Management and Owners should undergo AML Awareness, Governance and Risk Framework, Latest updates on laws and regulations, minimum once in a year. These trainings shall be organized through the external agencies.

7.2. Topics:

The topics for AML & CTF training should focus on the different levels of employees, i.e., whether the employee is a customer facing employee, a supervisor, or a clerical employee.

The medium and topics of training should be made available as per the nature of the role an employee is working in. The training mediums may be in the form of classroom sessions, circulars, e-learning modules, corridor specific trainings, role plays.

The topics should include:

7.2.1 General information:
Background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important.

7.2.2 Legal framework:
How the AML Laws apply to institutions and their employees.

7.2.3 Responsibility:
Responsibility of the employees under local laws and regulations for obtaining sufficient evidence of identity, recognizing, and reporting knowledge or suspicion of money laundering and terrorist financing.

7.2.4 Penalties:
For Anti-Money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.

7.2.5 Other Topics:
How to react when faced with a suspicious client or transaction & Procedure for reporting of suspicious transactions, how to respond to customers who want to circumvent reporting requirements and Internal policies, such as customer identification and verification procedures and:

- CDD policies.
- What are the legal recordkeeping requirements?
- Red flags.
- Suspicious transaction reporting requirements.
- Duties and accountability of employees.
- Fraud Prevention.
- Tipping off.

Training Assessment

- All company employees have to complete the annual AML CFT training as pert heir function/department requirements listed above.
- The AML/CFT training modules can be prepared by the Compliance Officer in house or can be outsourced to a firm specializing in AML/CFT training.
- As part of the internal compliance monitoring the Compliance Officer will decide the criterion for completion of the AML/CFT Training and design the training module accordingly.

8. RECORD KEEPING:

Records should be kept and made available to Regulatory examiners and for investigation for a minimum of 5 years. The objective for records keeping is to ensure that the company can provide thebasic information to reconstruct the transaction undertaken, at the request of the relevant authorities.

8.1 Document retention:

The records prepared and maintained by the company must be such that:

- The requirements of the law and expectations of the regulator or the supervisor are fully met; and Auditors, reporting accountants, and regulators or supervisors are able to assess the effectiveness of Promise Gold Refinery FZC .'s AML/CFT policies and procedures.
- Any transaction or instruction conducted through the NBFI on behalf of any individual customer can be reconstructed.
- Any customer or underlying beneficial owner can be properly identified.
- All suspicious transaction reports received internally, and those submitted to the financial intelligence unit, can be identified; and
- The company can meet, within the required time frame, any inquiries or court orders from the appropriate law enforcement agencies.

8.2. How long should records be retained?

The minimum periods for which records must be maintained to comply with the requirements of the law are outlined in the following table.

Type of Account	Length of Retention
Account Opening records and documentary evidence of Identity	At least 5 years after Account Closure.
Account ledger records.	At least 5 years
Individual transaction records.	At least 5 years
Results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, usual large transactions).	At least 5 years
Information after the account has been closed orafter the last transaction.	At least 5 years
AML Training registers.	At least 5 years

Records relating to a customer's identity must be retained for at least 5 years from the date of closure of business with the client. The date on which the relationship with a customer end is the date of:

- Carrying out a one-off transaction or the last in the series of transactions; or
- Ending of the business relationship, that is, the closing of an account.

9. FINES AND PENALTIES

As per Federal Decree – Law (20) of 2018.

The Regulator has the authority to impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in casethey violate the present Decree-Law and its Implementing Regulation:

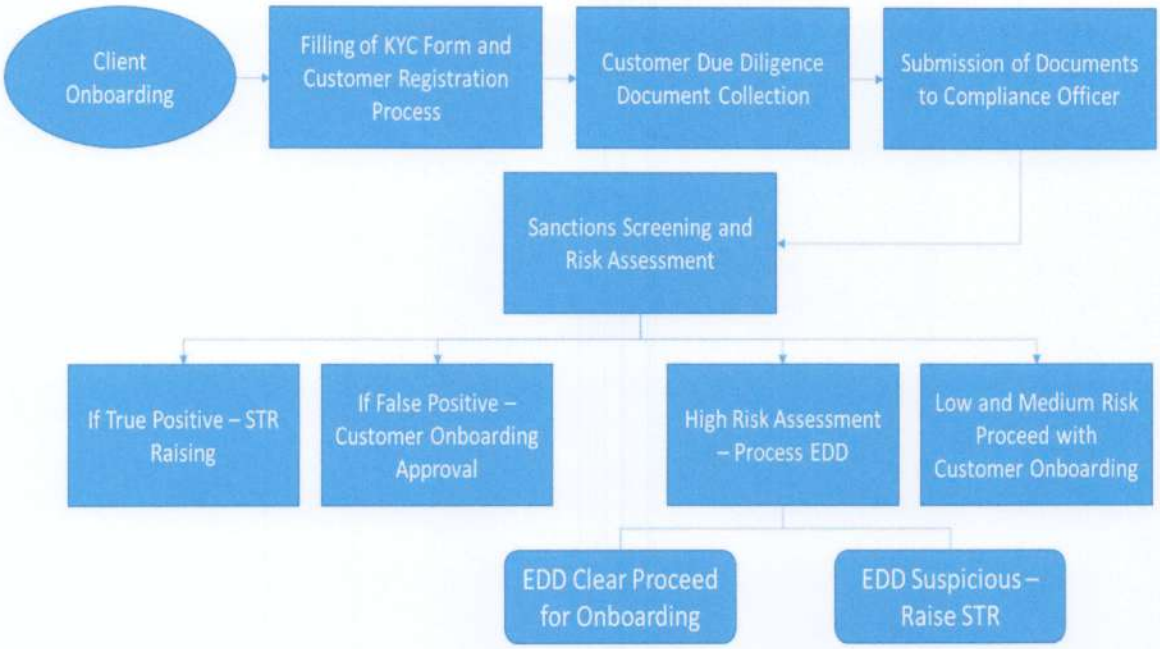
- Warning.
- Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (fivemillion dirham) for each violation.
- Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
- Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointmentof temporary inspector.
- Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
- Arrest or restrict the activity or the profession for a period to be determined by the supervisoryauthority.
- Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.

https://www.moj.gov.ae/Content/Userfiles/Assets/Documents/e6941183.pdf

10. ANNEXURE

10.1 Flow Chart - Onboarding of Customer Process



Customer Due-Diligence:

As the company is engaged in bullion and precious metals related products, the company should consider the following while conducting business with any entity. The KYC norms revolve around the following key elements:

1. **Risk Classification -** Based on type of Customer and nature of business, the customers are classified into High, Medium & Low risk categories. Enhanced due diligence is undertaken on all high-risk accounts by obtaining additional identification documents and information regarding the customer, their business and financial activities.

- **Customer Risk:** Whether the counterparty or customer is a physical person, a legal person, or a legal arrangement, if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a Political Exposed Person (PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate.

- **Geographic Risk:** Country of origin of the product, particularly in relation to whether the country is a known production or trading hub for the type of precious Metals and Stone; has adequate regulations and controls (for example, is a participant in the Kimberley Process Certification Scheme (KPCS) for rough diamonds); is a High-Risk Country (e.g., is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist Organizations). Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country).

- **Channel Risk:** Channel by which the counterparty/customer is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy).

2. **Customer Acceptance Policy and identification procedures** - Identifying the customer and verifying the legal status by using reliable, independent source documents, data and other information.

3. **On-going Monitoring Process & Reporting** – All client activity monitored on an ongoing basis to ensure that the transactions being conducted are consistent with the Company's knowledge of the client, its business and risk profile which would be, reported to management for appropriate decision and action.

4. **Preliminary checks for On-Boarding Customers:** The Front Office (FO), prior to entering into business with any Client must perform certain mandatory checks from the Compliance perspective. This is done in order to establish that the Client is not involved in any adverse activities in relation to, directly or indirectly, the Client's business and use/source of funds. The Front Office performs these preliminary checks before the Client file is completed and submitted to Compliance for approval

   - **AML/KYC Check:** The Front Office must complete a thorough check on the Client with respect to Anti-Money Laundering (AML) issues and a thorough Know Your Customer (KYC) check.
   - **Ownership:** FO must identify threadbare all the Beneficial Owners and Shareholders for the prospect. Sometimes this may require a detailed understanding of ownership structures. Nevertheless, this is essential prior to onboarding.
   - **Executive Powers:** FO also needs to identify all the persons with Executive Powers like Directors, Shareholders and Authorized signatories. In other words, it is important to know how owners have passed on Managerial authority to the executives who run the client on a day-to-day basis.

5. **Collection of documents:** Several documents and worksheets need to be collected, collated, certified, and signed off in order to be able to submit a completed file to Compliance for an approval to on-board a client. Once FO is satisfied with the information obtained from the above three checks. the next step is to obtain certain official documents from the Client in order to complete the Client file for submission to Compliance. These documents include;

   - **Memorandum of Association (MoA) / Articles of Association (AoA):** FO needs to obtain a copy of the Client entity's MoA/AoA in order to determine the company clauses and articles during origination. Prospect must be informed any changes in the MoA/AoA, must be immediately communicated to
   - **List of Beneficial Owners and Shareholders:** The FO must obtain the entire list of Beneficial Owners and Shareholders of the Client entity from top to bottom. This list will be available either in the MoA/AoA depending on country on incorporation.
   - **Certificate of Incorporation (CoI) / Trade License (TL):** The Client must provide FO with its CoI or any such equivalent official document. The FO will also require the Client's TL which must be certified and including renewal date. The Trade License would reveal where the Client is registered and under what legislation or how it is regulated. The TL provides information on the Ownership and management with respect to the operations of the Company.
   - **List of Directors and Authorized Signatories:** The List of Directors should contain Names of Directors, Country of Residence, Nationality of Directors, Partners and of the Members of the Governing Body. The Client must provide with a confirmation by letter on a periodic basis and especially at any time of change in the List of Directors, Partners and/or Beneficial Owners. A certified copy specifying who is authorized to act on behalf of the client and of the board resolution authorizing the signatories to operate the account must also be provided to. This Authorized

signatory list should be certified by client and a written intimation about changes to this Signatory list must be communicated to immediately, as and when such changes occur.

- **Certified Identification:** Certified Identification (Passport) for all Directors, all Partners, all Shareholders and all Authorized Signatories is required along with the proof of address for 2 Directors and 2 Authorized Signatories. Identifications in the form of Government –issued ID/Driver's License showing address or any other Valid Identification may be accepted. **Utility Bill/Local Authority Tax Bill or Bank/Building Society/Credit Union/Mortgage Statement may also be sufficient. All bills must be dated within 3 months of the start date of on-boarding process. These IDs provide the Residential Proof that substantiates the Country of Residence.
- **World Check or relevant paid sanctions sources, Google News Searches and Passport Check:** Carry out thorough check on all Directors, Shareholders, Beneficial Owners, Authorized Signatories, and major suppliers of Client on World Check. A similar search is also to be done on Google News. Record any adverse information and report to Senior Management and Compliance Officer. This check provides ALL relevant and irrelevant information that might prove quintessential to with respect to the risk associated with doing business with prospective Client. World Check picks up and highlights all adverse information and identifies Politically Exposed Persons (PEPs). FO must also perform a Passport Check, which is part of the World Check tool, on all individuals for whom Passport ID has been acquired to ensure authentication of identity and prevent forgery. Passport Check is essential in identifying if any Passport Copy provided by the prospective Client is valid/authentic or fake/forged. PEP information must be noted for signoff by Head of Operations
- Financials of the Client: FO must obtain as mentioned before during the process of AML/KYC, the financials of the Client entity. In order to be able to correctly identify the Client's position on the Source of Funds and Wealth, at least previous 3 years Balance Sheets must be obtained from the Client.

6. **Documents to be prepared by FO for Onboarding:** Certain forms need to be prepared and completed in order to add to the Client file for submission to Compliance for an approval to on-board the Client. After the completion of this process, the Client file is submitted to Compliance for approval to on-board.

   Risk Assessment Worksheet: Completed & signed off by Front Office. If PEP (Politically Exposed Person) is identified, contact Compliance for guidance. Based on the assessed risk score for the client, corresponding Due Diligence must be performed:

   - **LOW RISK** – Simplified Due Diligence
   - **MEDIUM RISK** - Standard Due Diligence
   - **HIGH RISK-** Enhanced Due Diligence

   The objective of the Risk Assessment Worksheet is to be able to assess the different levels and fronts at which the company faces risks with regard to doing business with the concerned prospective Client. (Supporting Document set-1)

   - Account Opening Form: Completed & signed off by Front Office. (Supporting Document set-1
   - KYC Checklist: Prepare and complete a KYC Checklist. Completed and signed off by respective Client Relationship Manager. The date for further review must also be mentioned.
   - (Supporting Document set-1)
   - Senior Management KYC Review Form: Prepare and complete the Senior Management KYC Review Form. Include all adverse information, if found, in the form. The form must be approved by the Senior Business Manager, Compliance & if necessary escalated to the Head of operations.

10.2. Risk Assessment Process for Money Laundering – Individual

Customer	Category 1	Category 2	High Risk	Medium Risk	Low Risk
Individual	Residential Status	Resident Local			
		Resident Expat			
		Non-Resident			
	Nationality	Low			
		Medium			
		High			
	Income Status	Salaried - Investment Matching to Profile			
		Salaried - Investment Not Matching to Profile			
		Business - Investment Matching to Profile			
		Business - Investment Not Matching to Profile			
Delivery Channel	Cash	Cash Transaction			
	ATM Deposit	ATM Deposit Transaction			
	Bank Transfer	Bank Transfer from Own Account and Customer Risk is Low			
		Bank Transfer from Own Account and Customer Risk is Medium			
		Bank Transfer from Own Account and Customer Risk is High			
		Bank Transfer from Third Party Account			

Country Risk Classifications

Lower	Lower - Med	Medium	Med - Higher	High
80 - 100	70 - 80	60 - 70	50 - 60	<50

ABBREVIATIONS LIST:

Term	Definition
Beneficial Owner:	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.
Business Relationship	Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them.
Committee:	National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations.
Competent Authorities:	The competent government authorities in the State entrusted with the implementation of any provision of the Decree-Law and the present Decision.
Crime:	Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organizations.
Customer Due Diligence (CDD):	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 Decree-Law and this Decision.
Customer:	Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law (Articles 2 and 3 the Cabinet Resolution) with one of the Financial Institutions or Designated Nonfinancial Businesses and Professions.
Decree-Law (or "AML-CFT Law"):	Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.
Decision (or "AML-CFT Decision" or "Cabinet Decision"):	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.

Term	Definition
Designated Nonfinancial Businesses and Professions (DNFBPs):	Anyone who conducts one or several of the commercial or professional activities defined in Article 3 of the Cabinet Decision, being anyone who is engaged in the following trade or business activities: 1. Brokers and real estate agents when they conclude operations for the benefit of their Customers with respect to the purchase and sale of real estate 2. Dealers in precious metals and precious stones in carrying out any single cash transaction or several transactions that appear to be interrelated or equal to more than AED 55,000. 3. Lawyers, notaries, and other independent legal professionals and independent accountants, when preparing, conducting or executing financial transactions for their Customers in respect of the following activities: (a) Purchase and sale of real estate. (b) Management of funds owned by the Customer. (c) Management of bank accounts, saving accounts or securities accounts. (d) Organising contributions for the establishment, operation or management of companies. (e) Creating, operating or managing legal persons or Legal Arrangements. (f) Selling and buying commercial entities. 4. Providers of corporate services and trusts upon performing or executing a transaction on the behalf of their Customers in respect of the following activities: (a) Acting as an agent in the creation or establishment of legal persons. (b) Working as or equipping another person to serve as director or secretary of a company, as a partner or in a similar position in a legal person. (c) Providing a registered office, work address, residence, correspondence address or administrative address of a legal person or Legal Arrangement. (d) Performing work or equipping another person to act as a trustee for a direct Trust or to perform a similar function in favor of another form of Legal Arrangement. (e) Working or equipping another person to act as a nominal shareholder in favor of another person. 5. Other professions and activities which shall be determined by a decision of the Minister

Term	Definition
Egmont Group:	The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/FT).
FATF:	The Financial Action Task Force is an inter- governmental body that 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.
FSRBs:	FATF-Style Regional Bodies are regional intergovernmental Organizations which promote and assess the implementation of internationally accepted AML/CFT policies and regulations.
Financial Group:	A group of financial institutions that consists of holding companies or other legal persons exercising the control over the rest of the group and coordinating functions for the application of supervision on the group, branch, and subsidiary level, in accordance with the international core principles for financial supervision, and AML/CFT policies and procedures.
Financial Institution:	Anyone who conducts one or several of the financial activities or operations of /or on behalf of a customer.
Financial Transactions or Activities:	Any activity or transaction defined in Article (2) of the Cabinet Decision.
Financing of Illegal Organizations:	Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or members.
Financing of Terrorism:	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014 on combating terrorism offences.
FIU:	Financial Intelligence Unit.
Funds:	Assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.

Term	Definition
High Risk Customer:	A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority.
Illegal Organizations:	Organizations whose establishment is criminalized or which exercise a criminalized activity.
Intermediary Account:	Corresponding account used directly by a third party to conduct a transaction on its own behalf.
Law Enforcement Authorities:	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidences on the crimes including AML/CFT crimes and financing illegal Organizations.
Legal Arrangement:	A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as Trusts or other similar arrangements.
MENAFATF:	MENAFATF is 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 international AML/CFT standards. The UAE is one of the founding members of MENAFATF.
Means:	Any means used or intended to be used for the commitment of an offence or felony.
Minister:	Minister of Finance
Money Laundering:	Any of the acts mentioned in Clause (1) of Article (2) of the Decree-Law.
Non-Profit Organizations (NPOs):	Any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit Legal Arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities.

Term	Definition
Politically Exposed Persons (PEPs):	Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States 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 organization or any prominent function within such an organization; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.
Predicate Offense:	Any act constituting an offense or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.
Proceeds:	Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
RBA:	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk.
Registrar:	Entity in charge of supervising the register of commercial names for all types of establishments registered in the State.
Sanctions Committee:	The UN Security Council Committee established as per resolution nos. 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.
Sanctions List:	A list wherein individuals and terrorist Organizations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee are listed, along with their personal data and the reasons for Listing.
Settlor:	A natural or legal person who transfers the control of his funds to a Trustee under a document.

Term	Definition
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
State:	United Arab Emirates
Supervised institutions:	Financial institutions (DNFBPs) and Designated Non- Financial Businesses and Professions (DNFBPs) which fall under the scope of Federal Decree-Law No. (20) of 2018 on Facing Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, and of 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.
Supervisory Authority:	Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and non-profit Organizations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations.
Suspicious Transactions:	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanour or felony or related to the Financing of Terrorism or of illegal Organizations, whether committed or attempted.
TFS:	Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.
Transaction (incl Commercial Transaction):	Any business of either dealing, structuring, advising, drafting, appearing, arranging for funding or investing, preparing documentation or disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation.
Trust:	A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.

Abbreviation	Full form
DNFPB	Designated Non-Financial Business
PMS	Precious Metal and Stones
ML/TF	Money Laundering/Terrorist Financing
FIU	Financial Intelligence Unit
PEP	Political Exposed Person
KPCS	Kimberley Process Certification Scheme
UBO	Ultimate Beneficiary Owner
EDD	Enhanced Due Diligence
SAR	Suspicious Activity Report
DPMS	Dealers in Precious Metals and Stones
CDD	Customer Due Diligence
NBFI	Non-Banking Financial Institutions
FATF	Financial Action Task Force
BOD	Board of Directors
NOC	No Objection Certificate
AML Def List	AML Deficiency List