PEAK INTERNATIONAL TRADING CO. LLC

Anti-Money Laundering and Combating Financing of Terrorism and Counter Proliferation Financing, And Targeted Financial Sanction (AML/CFT/CPF & TFS) Policy, Procedures and Controls.

Version 2.0 January 2025

CONTENTS

1. DOCUMENT INFORMATION

Document Title	Anti-Money Laundering, Combating Financing of Terrorism, Counter Proliferation Financing and Targeted Financial Sanctions (AML/CFT/CPF and TFS) Policies, Procedures, and Controls.
Document Version	2.0
Effective From	January 2025
Prepared By	Name: Vishnu Shaji Designation: Compliance Officer Signature: 
Reviewed & Approved By	Name: Sercan Samet Onder Designation: Owner Signature  

Company Stamp

2. DOCUMENT REVISION HISTORY

Date	Version	Author	Description
May 2024	1.0	General Manager	AML policy
Jan 2025	2.0	Compliance Officer	AML/CFT/CPF&TFS Policy, Procedures and Controls implemented as per the MOE guidelines, notices and circular.

3. STANDARDS, GUIDELINES, NOTICES & APPLICABLE LAWS

This policy and procedures are created based on the following resources;

S.No.	Details
1	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 Organisations.

2	Federal Decree No. 20 of 2018 on anti-Money Laundering and Countering the Financing of Terrorism.
3	Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. (20) 2018 on anti-money laundering and combating the financing of terrorism and illegal organizations.
4	Cabinet Resolution No (24) of 2022 Amending some provisions of Cabinet Resolution No (10) of 2019 On the Executive Regulations Of Federal Decree-Law No (20) of 2018 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations.
5	Cabinet Resolution No. (53) of 2021 Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Resolution No. (58) of 2020 Concerning the Regulation of Beneficial Owner Procedures.
6	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 that are Subject to the Supervision of the Ministry of Justice and the Ministry of Economy.
7	Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures.
8	Cabinet Decision No. (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.

4. GUIDELINES

S.No.	MOE Guidelines
1	Guidelines for Designated Non-Financial Businesses and Professions
2	Supplemental Guidance for Dealers in Precious Metals and Stones
3	Proliferation Finance Institutional Risk Assessment Guidance
4	Implementation Guide for DNFBPs on Customer Due Diligence (CDD)
5	Implementation Guide for DNFBPs on Customer Risk Assessment (CRA)

5. CIRCULARS

S.No.	CIRCULARS
1	Circular No. 4 of 2024 (29th October 2024) MOEC/AML/004/2024 Updated the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the counter-measures to be applied
2	Circular No. 3 of 2024 (1st July 2024) MOEC/AML/003/2024 has updated the list of High-Risk Jurisdictions subject to Call for Action and the list of Jurisdictions under Increased Monitoring.
3	Circular No. 1 of 2024 has updated the list of High-Risk Jurisdictions subject to Call for Action and the list of Jurisdictions under Increased Monitoring.
4	Circular No. (4) of 2023 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and update the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
5	Circular No. (3) of 2023 - Update the list of High-Risk countries/ Jurisdictions subject to a Call for Action and list of countries/ jurisdictions under Increased Monitoring, and update the counter-measures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
6	Circular No. (1) of 2023 update the list of high-risk Jurisdictions
7	Circular No. (2) of 2022 regarding Implementation of Targeted Financial Sanctions (TFS) on UNSCRs 1718 (2006) and 2231 (2015)
8	Circular No. (6) of 2022 regarding Update the list of High-Risk Jurisdictions subject to a Call for Action and list of Jurisdictions under Increased Monitoring, and update the counter-measures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
9	Circular No. (3) of 2022 (Updated List of High-Risk Countries)
10	Circular No. (1) of 2022 (results of the United Arab Emirates Money Laundering & Terrorist Financing Risk Assessment)
11	Circular No. (9) of 2021 regarding updating the list of high-risk countries
12	Circular No. (8) of 2021 (GoAML Reporting Requirements)
13	Circular No. (6) of 2021 for High-Risk Country
14	Circular No. (5) of 2021 - Reference to our Notice No. 1/2020 dated 16/December/2020 regarding Targeted Financial Sanctions (TFS) Reporting

6. INTRODUCTION

DPMS: A dealer in PMS (Precious Metal Stone) may be considered to be any natural or legal person (or legal arrangement), or their employee or representative, who engages, as a regular component of their business activities, in the production and/or trade of precious metals or precious stones, whether in raw, cut, polished, or elaborated (mounted or fashioned) form. Production and/or trade in this context includes any of the following acts involving raw/rough or processed/finished PMS:

- Extraction (whether by mining or other method), refining, cutting, polishing or fabrication;
- Import or export;
- Purchase, sale, re-purchase or re-sale (whether in primary, secondary, or scrap markets);
- Barter, exchange, or other form of transfer of ownership;
- Loan or lease arrangements (e.g., sale-leaseback, consignment, or memorandum sales);
- Possession (whether permanent or temporary, for example, as part of a fiduciary, warehousing, collateral, or other safekeeping arrangement; or under contract for a specific purpose such as cutting, polishing, refining, casting or fabrication services).

DPMS AML/CFT Obligation: 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 Organisations (the "AML-CFT Decision") identifies dealers in precious metals and precious stones (DPMS) as Designated Non-Financial Business and Professions (DNFBPs), when they engage in carrying out any single monetary transaction, or several transactions which appear to be interrelated, whose value is equal to or greater than AED 55,000, and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates.

This policy will be useful to:

- New employees are encouraged to acquaint themselves with the policies and procedures concerning Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and guidelines related to Illegal organizations.
- Current employees fulfilling their duties and responsibilities.
- Correspondence banks, agents and partners to understand Anti-Money Laundering and Combating Financing Terrorism Policies and Procedures adopted by the Company.

7. ABOUT THE COMPANY

At Peak International Trading, we have years of experience in the field of gold and precious metals-stone trading. Our mission is to provide reliable and high-quality services to our customers. We aim to satisfy you with tailored solutions that meet your needs in the gold and precious metals-stone trade. With our customer-centric approach, we are here to offer you the best service.

Our company, which started its operations in Dubai this year, has a deep expertise in the trade of gold and precious metals-stones. We are dedicated to providing our customers with the highest quality products and services.

- Precious Metals - Stones
- Jewelry, diamond and gemstone trade
- Investment guidance and analysis.

Expertise
Our extensive knowledge in the gold and precious metals-stone trade ensures trustworthy and well-informed transactions.

Reliability
Our well-established reputation in the precious metal industry is a testament to our reliability. Clients can place their trust in us with confidence.

Transparency
We prioritize open and honest communication, providing clients with a clear understanding of every transaction

Quality
We offer top-tier products, assuring customers the finest gold and precious metals-stones.

Efficiency
We're committed to swift service, reducing delays for confident transactions.

Customer-Centric Approach
Our focus on client satisfaction means tailor-made solutions that meet their unique needs and preferences.

Our Mission
Our mission is to responsibly source, refine, and distribute precious metals of the highest quality to meet the diverse needs of our customers. We aim to ensure the integrity and purity of our products, provide exceptional service and value, and contribute to the long-term growth and stability of the precious metal industry. Through innovation, sustainability, and customer-centricity, we strive to be a trusted partner in preserving and maximizing the value of precious metals for investors, collectors, and industries worldwide.

Our Vision
Our vision is to be the leading global provider of precious metals, setting the standard for integrity, innovation, and sustainability. We aim to empower individuals, investors, and industries with reliable access to high-quality precious metals, while fostering long-term growth and delivering exceptional value.

8. OUR COMMITTMENT

Peak International Trading CO LLC hereinafter referred to as the “Company”, as a Designated Non-Financial Business or Profession (DNFBP), places significant importance on adhering to the UAE's Anti-Money Laundering (AML) Compliance requirements as prescribed by the Ministry of Economy. These requirements serve as an important framework for preventing and detecting money laundering activities within the DPMS industry.

The Company has established a comprehensive system and robust procedures designed to safeguard against potential involvement in illicit financial transactions. Recognizing the paramount importance of maintaining transparency and compliance, the Company endeavors to cultivate a trustworthy environment among its clients and stakeholders, thereby contributing to the overall integrity of the UAE's financial and commercial sectors.

The Company's AML compliance measures encompass stringent due diligence processes for customer onboarding and continuous monitoring of client transactions. Before initiating any business relationship, thorough customer due diligence is conducted, including verification of identity and background checks, alongside an assessment of transactional activities. This meticulous process enables the identification and mitigation of potential risks associated with money laundering or terrorist financing.

Maintaining a vigilant approach to ongoing monitoring, the Company regularly reviews and analyzes client transactions to promptly identify any suspicious activities or unusual patterns that may indicate potential money laundering. This proactive monitoring empowers the Company to take requisite actions, such as reporting suspicious transactions to the relevant authorities, in strict adherence to regulatory guidelines.

Moreover, the Company fosters a robust collaboration with regulatory authorities and extends full cooperation during inspections and audits. Through active engagement with relevant authorities, the Company demonstrates its unwavering commitment to upholding the highest standards of AML compliance.

9. PURPOSE OF THE POLICY

The purpose of the policy is to effectively implement the key principles of AML/CFT/CPF & TFS laws and regulations, in line with Ministry of Economy / Committee for Commodities Subject to Import & Export Control / Financial Intelligence Unit, by educating our employees to act as the first line of defense in combating money laundering activities.

The Company accepts only those customers whose source of fund can be reasonably established as legitimate and who do not pose any risk (actual or potential) to the company’s reputation. and;

a) Engage only in legitimate business abiding by all relevant rules and regulations which apply to our activities.

b) Maintain the highest ethical and moral standards.

c) Operate always under best practice exercising due-care and all necessary due-diligence.

d) Aim to establish long-term relationships with our immediate clients.

10. APPLICABILITY

This policy applies to all employees including Senior Management of the Company. Any breach of the policy by employees or branches constitutes a disciplinary offense. The Company reserves the right to take any additional action it deems fit, at its sole discretion, to ensure diligent and proper implementation and enforcement of the policy.

11. REVIEW & APPROVAL

The AML/CFT/CPF & TFS Policy and Procedures shall be reviewed and updated, annually at a minimum, to make it consistent with all applicable Laws, Regulations, Notices, the Standards and other international best practices and to make it effective in mitigating the existing as well as emerging ML/FT/PF risks.

The review would be done by the compliance officer and approve by the Owner/Manager.

The policies would be reviewed annually as well as in the event of the following:

- Change in regulatory guidelines of Ministry of Economy / Committee for Commodities Subject to Import & Export Control / Financial Intelligence Unit of the UAE as well as any other relevant authorities.
- Change in business profile/ product mix due to change in business model or market conditions.

Part - I

OVERVIEW

12. OVERVIEW OF THE AML/CFT LEGAL, REGULATORY, AND NATIONAL STRATEGY FRAMEWORKS OF THE UNITED ARAB EMIRATES

12.1. NATIONAL LEGISLATIVE AND REGULATORY FRAMEWORK

The legal and regulatory structure of the UAE is comprised of a matrix of federal civil, commercial and criminal laws and regulations, together with the various regulatory and Supervisory Authorities responsible for their implementation and enforcement, and various local civil and commercial legislative and regulatory frameworks in the Financial and Commercial Free Zones. As criminal legislation is under federal jurisdiction throughout the State, including the Financial and Commercial Free Zones, the crimes of money laundering, the financing of terrorism, and the financing of illegal organisations are covered under federal criminal statutes and the federal penal code. Likewise, federal legislation and implementing regulations on the combating of these crimes are in force throughout the UAE, including the Financial and Commercial Free Zones. Their implementation and enforcement are the responsibility of the relevant regulatory and Supervisory Authorities in either the federal or local jurisdictions.

The principal AML/CFT legislation within the State is Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (the "AML-CFT Law" or "the Law") and implementing regulation, 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 Organisations (the "AML-CFT Decision" or "the Cabinet Decision"

The UAE recently issued Cabinet UBO Resolution No. 58 of 2020 on the Regulation of the Procedures of the Real Beneficiary (UBO Resolution) which came into effect on 28 August 2020 and replaced Cabinet Resolution No. 34 of 2020 issued earlier this year.

DNFBPs licensed and operating from Financial Free Zones should refer to the regulations governing beneficial ownership and control issued by their relevant Financial Free Zone authority.

The UBO Resolution introduces the requirement for a beneficial ownership register in the UAE mainland and unify the minimum disclosure requirements for corporate entities incorporated in the UAE mainland and in the non-financial free zones.

12.2. INTERNATIONAL LEGISLATIVE AND REGULATORY FRAMEWORK

The AML/CFT legislative and regulatory framework is part of a larger international AML/CFT legislative and regulatory framework made up of a system of intergovernmental legislative bodies and international and regional regulatory organisations. On the basis of international treaties and conventions in relation to combating money laundering, the financing of terrorism and the prevention and suppression of the proliferation of weapons of mass destruction, intergovernmental legislative bodies create laws at the international level, which participating member countries then transpose into their national counterparts. In parallel, international and regional regulatory organisations develop policies and recommend, assess and monitor the implementation by participating member countries of international regulatory standards in respect of AML/CFT.

12.2.1. THE UNITED NATIONS (UN)

The UN is the international organisation with the broadest range of membership. Founded in October of 1945, there are currently 191 member states of the UN from throughout the world. 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).

12.2.2. THE UNITED NATIONS SECURITY COUNCIL (UNSC)

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and has primary responsibility for the maintenance of international peace and security. The Security Council sanctions regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counterterrorism. These regimes include measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.

12.2.3. THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an intergovernmental body established in 1989, which sets international standards on anti-money laundering (AML) and countering the financing of terrorism (CFT) and proliferation (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards requires the implementation of targeted financial sanctions (TFS) to comply with the UN Security Council Resolutions (UNSCRs) relating to the prevention and suppression of Terrorism, Terrorism Financing (TF), and Proliferation Financing (PF) 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. FATF also monitors the implementation of its standards, the 40 FATF Recommendations and 11 Immediate Outcomes, by its members and members of FSRBs, ensures that the 'FATF Methodology' for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems is properly applied.

12.2.4. THE MIDDLE EAST AND NORTH AFRICA FINANCIAL ACTION TASK FORCE (MENAFATF)

Recognizing the FATF 40 Recommendations on Combating Money Laundering and the Financing of Terrorism and Proliferation, and the related UN Conventions and UN Security Council Resolutions, as the worldwide-accepted international standards in the fight against money laundering and the financing of terrorism and proliferation, 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 MENAFATF.

12.2.5. THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

In 1995, a number of FIUs began working together and formed the Egmont Group of Financial Intelligence Units (Egmont Group) (named for the location of its first meeting at the Egmont-Arenberg Palace in Brussels). The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML/CFT programs and to coordinate AML/CFT initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

12.2.6. THE MINISTRY OF ECONOMY

The Ministry of Economy, as the supervisory authority, is entrusted with the supervision of the 'Designated Non-financial Businesses and Professions' (DNFBPs) sector at the state level and commercial free zones in order to combat money laundering and financing of terrorism. It is committed to developing a strong regulatory framework and providing a safe environment for organisations, companies, and DNFBPs to work according to international best practices. It also contributes towards raising the competitiveness of the state's economic, investment and financial environment, building an attractive business and investment climate within various sectors, and creating a balanced, flexible and sustainable future economic model. The priorities include providing all possible forms of knowledge, guidance and training support for Designated Non-financial Businesses and Professions, and raising their level of awareness to be able to fulfil their commitments, in partnership with various economic sectors. The main objective of the efforts of the Ministry of Economy at the international level is to raise the level of compliance with international requirements and maintain the top position and positive reputation of the national economy in global markets as well as with all countries and international partner organisations.

12.2.7. THE EXECUTIVE OFFICE FOR CONTROL AND NON-PROLIFERATION (EOCN)

The Executive Office for Control and Non-Proliferation (EOCN) plays an active role in implementing export control besides curbing the proliferation of weapons of mass destruction with relevant associated technology, based on policies, legislations and partnerships domestically and internationally. The EOCN was established in the United Arab Emirates in 2009 as a body responsible for implementing the provisions of Federal Decree Law No. (43) of 2021 On the Commodities Subject to Non-Proliferation which replaces Federal Law No. (13) of 2007 Concerning Commodities Subject to Control of Import and Export. This is for the aim of preventing the illegal and unauthorized circulation of dual-use goods that contribute to the production or development of weapons of mass destruction, along with their associated technology and means of delivery.

The Executive Office for Control and Non-Proliferation, in cooperation with the Ministry of Foreign Affairs and International Cooperation (MoFAIC) and other government agencies exert extreme efforts in following up the application of the resolutions and requirements of the United Nations Security Council and other relevant international and regional organizations. EOCN also coordinates to and supervises the application of targeted financial sanctions relating to terrorist lists system, as well as the implementation of Security Council resolutions on the prevention and

suppression of terrorism, its financing, the cessation of arms proliferation and financing, in addition to other relevant resolutions in coordination with competent stakeholders.

The Executive Office is the technical focal point for following up on the UAE's obligations in the Convention on the Prohibition of the Development, Production, Storage and Use of Chemical Weapons. This reflects the UAE Government's vision of maintaining security and stability inside and outside the country and promoting partnership with countries of the region and the rest of the world to be free of weapons of mass destruction.

12.2.8. AML/CFT NATIONAL STRATEGY FRAMEWORK

Money laundering and the financing of terrorism are crimes that threaten the security, stability and integrity of the global economic and financial system, and of society as a whole. The estimated volume of the proceeds of crime, including the financing of terrorism, that are laundered each year is between 2-5% of global GDP. Yet, by some estimates, the volume of criminal proceeds that are actually seized is in the range of only 2% of the total, while roughly only half of that amount eventually ends up being confiscated by competent judicial authorities. Combating money laundering and the financing of terrorist activities is therefore an urgent priority in the global fight against organised crime.

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organisations. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs, as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

As part of these efforts, the Competent Authorities of the UAE have taken a number of substantive actions, including among others:

- Enhancing the federal legislative and regulatory framework, embodied by the introduction of the new AML/CFT Law and Cabinet Decision, which incorporate the FATF standards;
- Conducting the National Risk Assessment (NRA) to identify and assess the ML/FT threats and inherent vulnerabilities to which the country is exposed, as well as to assess its capacity in regard to combating ML/FT at the national level;
- Formulating a National AML/CFT Strategy and Action Plan that incorporate the results of the NRA and which are designed to ensure the effective implementation, supervision, and continuous improvement of a national framework for the combating of ML/FT, as well as to provide the necessary strategic and tactical direction to the country’s public and private sector institutions in this regard.

The National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism of the United Arab Emirates is based on four pillars, each of which is associated with its own

strategic priorities. These strategic priorities in turn inform and shape the key initiatives of the country's National Action Plan on AML/CFT.

The pillars of the National Strategy, together with their strategic priorities are summarised in the table below:

National AML/CFT Strategic Pillars	Strategic Priorities
Legislative & Regulatory Measures	Increase effectiveness and efficiency of legislative and regulatory policies and ensure compliance.
Transparent Analysis of Intelligence	Leverage the use of financial databases and the development of information analysis systems to enhance the transparent analysis and dissemination of financial intelligence information.
Domestic and International Cooperation & Coordination	Promote the efficiency and effectiveness of domestic and international coordination and cooperation with regard to the availability and exchange of information.
Compliance and Law Enforcement	Ensure the effective investigation and prosecution of ML/FT crimes and the timely implementation of TFS.

The National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations has identified a number of key drivers of success in achieving the goals of the National AML/CFT Strategy. These include, among other things, ensuring:

- Effective coordination between the Financial Intelligence Unit, Law Enforcement Authorities, Public Prosecutors, Supervisory Authorities, and other Competent Authorities within the country;
- Effective compliance with the laws and regulations governing banking activities and other financial services;
- Awareness by DNFBPs of the relevant ML/FT risks facing the UAE in general, and their sectors in particular, as informed by the results of the NRA, as well as their awareness of their statutory obligations in regard to the management and mitigation of those risks.

12.2.9. TARGETED FINANCIAL SANCTIONS (TFS)

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and has primary responsibility for the maintenance of international peace and security. It has 15 Members, and each member has one vote. Under the Charter of the United Nations, all Member States of the UN are obligated to comply with the Security Council decisions.

The UNSC holds the capacity to take action seeking to maintain or restore international peace and security under Article 41 of Chapter VII of the Charter of the United Nations by imposing sanctioning measures. These measures encompass a broad range of enforcement options that do not involve the authorisation of the use of armed force, including interruption of economic relations, international communications, and diplomatic relations.

The Security Council sanctions regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counterterrorism. These regimes include measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.

In addition, the Financial Action Task Force (FATF), an inter-governmental body responsible for setting international standards on anti-money laundering (AML) and countering the financing of terrorism (CFT) and proliferation (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards, requires the implementation of targeted financial sanctions (TFS) to comply with the UN Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism, terrorism financing, and proliferation financing.

The United Arab Emirates (UAE), as a member of the United Nations, is committed to implementing UNSCRs, including those related to the UN's sanctions regimes. Consequently, through the Cabinet Decision No. 74 of 2020, the UAE is implementing relevant UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, in particular relating to TFS. Persons should note that, in accordance with the laws of the UAE, the UAE Government also applies TFS by publishing a Local Terrorist List in accordance with UNSCR 1373 (2001).

12.2.9.A) TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING

The term terrorist financing includes the provision of funds or assets to commit terrorist activities. This term includes providing food, lodging, training, and making means available such as transportation and communication equipment. Such financing can occur with money or in kind, and funds involved can be from legal or illegal sources.

The terrorist financing methods outlined which compiles information from documents developed by the UNSC, the United Nations Office on Drugs and Crime (UNODC), and the Financial Action Task Force (FATF).

Terrorist Financing Methods

- Banking Services
    - Continued access to bank accounts by foreign terrorist fighters
- Money Remitters
- Exchange Houses
- Hawala and Other Similar Service Providers (HOSSP)
    - Funds Sent to Boko Haram
    - Funds Sent to ISIL In Afghanistan
    - Funds Sent to Houthies In Yemen
- Online Payment Facilities
    - Fundraising Through the Internet

    - Online Financial Accounts Used for Fundraising
    - The Use of Social Media and Telegram Platforms to Promote Terrorist Activities

- The Misuse of Non-Profit Organizations (NPOs)
    - Support for Recruitment of Foreign Terrorist Fighters
    - NPO Affiliation with a Terrorist Entity
    - Donations to NPOs Affiliated with Terrorist Groups
- Cash Smuggling
- Smuggling of Gold
    - Cash Couriers
- Circumventing Sanctions Through Trade
    - Trade of Communication Devises
    - Trade of Natural Resources
    - Trade of Oil and Derivates
    - Trade of Charcoal from Somalia
- The Misuse of Legal Entities
- The Use of Virtual Assets to Support TF Groups.
    - Transferring funds via Bitcoin
    - Use of Virtual Assets Ethnically or Racially Motivated Terrorist Financing
    - Promotion of virtual currency to fund terrorism

12.2.9.B) TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION OF WMD

Recommendation 7 of the FATF Standards requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs or resolutions). Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD). Immediate Outcome 11 and certain elements of Immediate Outcome 1 relating to national cooperation and coordination aim to measure how effective countries are implementing these Recommendations.

The United Nations Security Council (UNSC or UN Security Council) has a two-tiered approach to counter proliferation financing through resolutions made under Chapter VII of the UN Charter and thereby imposing mandatory obligations for UN Member States:

- Global Approach Under UNSCR 1540 (2004) and Its Successor Resolutions

- Country-Specific Approach Under UNSCR 1718 (2006) And UNSCR 2231 (2015) And Their (Future) Successor Resolutions

The following are cases of violations or evasion of the sanctions imposed by the UNSC related to the Nuclear Programme of the Democratic People's Republic of Korea (DPRK), as presented by the Panel of Experts pursuant to UNSCR 1874, between 2017 and 2020 ("the UN Panel of experts") and the UAE cases related to Proliferation Financing.

- The use of Banking Sector
    - Designated banks maintain representative offices and agents abroad
    - Financial activities of diplomatic and other personnel of the DPRK
    - Transfers through banks
    - Use of cash to circumvent US sanctions
- Cyberactivity targeting financial institutions
    - Operation "FASTCash"
    - Cyberattack on Cryptocurrency Exchange House
- Economic Resources
    - Oil Ship-To-Ship Transfers
    - Smuggling Petrochemicals
    - Nickel Wire
    - Carbon Fiber
- Trade-In Other Goods
    - Generator
    - Vibration Analysis Devises
- Misuse of Legal Entities or Arrangements
    - Purchasing Aircraft Equipment Through 3rd Party
    - DGS Marine
    - The GENCO/KOGEN Group
    - GENCO Network
    - The Glocom Group
    - Financial Operations Of Glocom/Pan Systems Pyongyang

12.2.9.A) WHAT ARE TFS?

The term targeted financial sanctions includes both asset freezing without delay and prohibition from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

Asset freezing without delay: Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes:

- The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access.
- The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

Prohibition from making funds or other assets or services available: This means the prohibition to provide funds or other assets to or render financial or other services to, any designated individual, entity, or group.

12.2.9.B) DURATION OF THESE MEASURES

Asset freezing and prohibition measures have no time limit: the funds or other assets remain frozen, and the prohibition from making funds or other assets or services available remains until the individual, entity, or group is removed from the Local Terrorist List or the UN Consolidated List or until there is a freezing cancellation decision made by a competent authority or the UNSC.

12.2.9.C) PURPOSE OF TFS

The purpose of TFS is to deny certain individuals, entities, or groups the means to violate international peace and security, support terrorism or finance the proliferation of weapons of mass destruction. To achieve this, it seeks to ensure that no funds or other assets or services of any kind are made available to designated persons for so long as they remain subject to the targeted financial sanctions measures.

TFS are implemented in the UAE pursuant to UNSCRs in relation to:

a. Terrorism And Terrorist Financing:

1	Islamic State in Iraq and the Levant (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities.	UNSCR 1267 (1999), 1989 (2011) and its successor resolutions
2	The Taliban, and associated individuals, groups, undertakings, and entities.	UNSCR 1988 (2011) and its successor resolutions

3	Any individual or entity included in the Local Terrorist List, pursuant to UNSCR 1373 (2001)	UNSCR 1373 (2001)

The Proliferation of Weapons Of Mass Destruction (WMD):

1	Democratic People's Republic of Korea (DPRK): nuclear-related, other weapons of mass destruction-related and ballistic missile-related programmes.	UNSCR 1718 (2006) and its successor resolutions
2	Islamic Republic of Iran: nuclear programme	UNSCR 2231 (2015)

b. Other UN Sanctions Regimes with TFS:

1	Somalia	UNSCR 1844 (2008)
2	Iraq	UNSCR 1483 (2003)
3	Democratic Republic of Congo (DRC)	UNSCR 1596 (2005) & UNSCR 1807
4	Related to the involvement of terrorist bombing in Beirut (2005) plus restrictive measures in relation to UNSCR 1701 (2006) on Lebanon UNSCR 1636 (2005) & UNSCR 1701 (2006)	UNSCR 1636 (2005) & UNSCR 1701 (2006)
5	Libya	UNSCR 1970 (2011)
6	Central African Republic	UNSCR 2127 (2013)
7	South Sudan	UNSCR 2206 (2015)
8	Mali	UNSCR 2374 (2017)
9	Yemen	UNSCR 2140 (2014)

12.2.9.D) WHERE TO FIND THE UPDATED SANCTIONS LISTS?

The information on designated individuals, entities, or groups in the Sanctions Lists is subject to change. The most recently updated information can be found in the following links:

- ✓ The UAE has a Local Terrorist List of all the sanctioned individuals, entities, or groups designated by the UAE Cabinet. The link to the Local Terrorist List can be found at the bottom of the Sanctions Implementation webpage on the Executive Office for Control & Non-Proliferation's (EOCN) website: https://www.uaeiec.gov.ae/en-us/un-page?p=2#

- ✓ The UNSC has a UN Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC. This link can be found on: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

12.2.9.E) WHO IS THE TARGET OF THESE MEASURES?

The freezing measures, including the prohibition of making funds or other assets or services available, apply to:

a) Any individual, entity, or group designated in the Local Terrorist List issued by the Federal Cabinet or designated by the UNSC in the UN Consolidated List.

b) Any entity, directly or indirectly owned or controlled by an individual, entity, or group designated under A.

c) Any individual or entity acting on behalf of or at the direction of any individual, entity, or group designated under A & B.

In cases where an asset is owned or controlled in part or in full by a designated individual, entity, or group and such asset continues to produce benefit, for example in the form of dividends or interest, the relevant portion of such benefit is also subject to freezing measures.

12.2.9.F) TARGETED FINANCIAL SANCTIONS AS PER FATF RECOMMENDATIONS

Terrorist Financing (TF)	Proliferation Financing (PF)
• ISIS & Al-Qaida UNSCR 1267, 1989 • The Taliban	• Democratic People's Republic of Korea (DPRK) UNSCR 1718 (2006)

UNSCR 1988 • UAE Local Terrorist List UNSCR 1373	• Islamic Republic of Iran UNSCR 2231 (2015)

12.2.9.G) OBLIGATIONS TO IMPLEMENT TFS

- Register
- Screen
- Implement TFS
- Internal Controls

12.2.9.H) REGISTER

Register at the Executive Office website to receive automated email notifications: https://www.uaeiec.gov.ae

This registration helps the Company to receive updated and timely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN List.

The Company registered with the EOCN TFS and following the regulatory requirements.

12.2.9.I) SCREEN

Undertake ongoing and daily checks to the databases to identify possible matches with names listed in the Sanctions Lists issued by the UN or the UAE Local Terrorist List:

- Existing customer databases.
- Names of parties to any transactions.
- Potential customers.
- Beneficial owners.
- Names of individuals or entities with direct or indirect relationships with them.
- Customers before conducting any transactions or entering a business relationship with any Person.
- Directors and/or agents acting on behalf of customers (including individuals with power of attorney)

Important: Initial screening must be performed PRIOR to the onboarding of a customer and/or facilitation of an occasional transaction. Thereafter, screening should be done daily at the institution's own initiative. The Sanctions Lists are continuously updated and available on the Executive Office's website and the UN website online.

Screening for Natural Person:

- Name
- Aliases
- Date of birth
- Nationality
- ID or passport information
- Last known address

For Legal Persons & Arrangements

- Name (s)
- Aliases
- Address of registration
- Address of branches
- Other information (Because many names are very common, you may find various potential matches. However, it does not necessarily mean that the individual or entity you are dealing with is subject to TFS)

12.2.9.J) IMPLEMENT TFS

There are two TFS Reports are required to report in the goAML portal

- Fund Freeze Report (FFR)
- Partial Name Match Report (PNMR)

Fund Freeze Report (FFR)

A confirmed match is identified, the Company must freeze without delay (within 24hrs) all funds and other assets and submit a FFR through goAML within five business days of implementing the freezing measures, along with all the necessary information and documents regarding the confirmed match and the freezing measures taken. The following information is obligatory when submitting an FFR:

- The full name of the 'confirmed match'. Attach ID documents of the 'confirmed match', such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.

- Amount of funds or other assets frozen (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach proof documents such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.

Partial Name Match Report (PNMR)

In case a partial name match is identified, the Company is required to suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a Partial Name Match Report (PNMR) through goAML, which will be received by the EOCN and the relevant Supervisory Authority. The Company must ensure all the necessary information and documents regarding the name match are submitted and maintain suspension measures related to the

partial name match until further instructions are received from EOCN via goAML on whether to cancel the suspension ('false positive') or implement freezing measures ('confirmed match'). The following information is obligatory when submitting a PNMR:

- The full name of the 'partial name match'. Attach ID documents of the 'partial name match', such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.

- Amount of funds or other assets suspended (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach documentary proof such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.

False Positive

A "False Positive" is a potential match to listed individuals, groups, or entities either due to the common nature of the name or due to ambiguous identifying data, which on examination proves not to be a confirmed or potential match.

Non-Compliance

- Violating UAE Cabinet 74 of 2020 can expose the Company to administrative penalties and criminal prosecutions including:

  - Increased scrutiny of future actions from the UAE Government.
  - Supervisory authority may determine a ban of certain individuals from employment within the relevant sectors for a period of time.
  - A suspension, restriction, or prohibition of activity, business, or profession causes either revocation or withdrawal of the business license.

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

  - Art. 60. Every natural or legal person shall immediately comply with the instructions issued by the Competent Authorities in the State concerning the implementation of the resolutions issued by UN Security Council.

12.2.9.K) INTERNAL CONTROLS

- The Company is having the appropriate internal controls to ensure compliance with the most recent publication of targeted financial sanctions of the UNSC Consolidated lists and the Local Lists.

- The Company is having the Internal controls and procedures to ensure compliance with the obligations arising from Cabinet Resolution 74/2020.

- The Company has implemented Policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action or any Other Measures as per provisions of Cabinet Resolution 74/2020.

- Identify the existing accounts, transactions, funds or other assets of designated individuals, entities, or groups.

- Conduct ongoing TFS training and awareness sessions to relevant employees and senior management.

- Adopt reasonable measures to consider beneficial owners, signatories, and powers of attorney with respect to accounts or transactions when searching for activities by designated individuals, entities, or groups.

13. HIGHLIGHTS OF KEY PROVISIONS AFFECTING THE COMPANY

The AML-CFT Law and the AML-CFT Decision contain numerous provisions setting out the rights and obligations of the Company as well as their senior managers and employees. This section highlights some of the key provisions affecting the Company that are of immediate concern. The Company reminded that it is their sole responsibility to adhere to all provisions of the AML-CFT Law, the AML-CFT Decision, and all regulatory notices, rulings and circulars affecting them.

13.1. SUMMARY OF MINIMUM STATUTORY OBLIGATIONS OF THE COMPANY

The AML-CFT Law and the AML-CFT Decision set out the minimum statutory obligations of the Company as follows:

- To identify, assess, understand risks.
- To define the scope of and take necessary due diligence measures.
- To appoint a compliance officer, with relevant qualification and expertise and in line with the requirements of the relevant Supervisory Authority.
- To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation.
- To put in place indicators to identify suspicious transactions.
- To report suspicious activity and cooperate with Competent Authorities.
- To maintain adequate records.

13.2. CONFIDENTIALITY AND DATA PROTECTION

The Company is obliged to report to the UAE's Financial Intelligence Unit (FIU) when they have reasonable grounds to suspect a transaction or funds representing all or some proceeds, or suspicion of their relationship to a Crime. In reporting the suspicions, we must maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

The confidentiality requirement does not pertain to communication within the Company or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of a Crime. However, under no circumstances the Company, or their managers or employees, permitted to inform a customer or the representative of a Business Relationship, either directly or indirectly, that a report has been made, under penalty of sanctions. This is the so-called "tipping off" requirement. This also extends to any related information that might be provided to the FIU or information that is being requested by the FIU.

The Company is not permitted to object to the statutory reporting of suspicions on the grounds of Customer confidentiality or data privacy, under penalty of sanctions. Moreover, data protection laws include provisions that allow the Company to report to the authorities.

13.3. PROTECTION AGAINST LIABILITY FOR REPORTING PERSONS

(AML-CFT Law Article 27; AML-CFT Decision Article 17.3)

The Company as well as their members, employees and authorized representatives, are protected by the relevant articles of the AML-CFT Law and AML-CFT Decision from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

13.4. STATUTORY PROHIBITIONS

(AML-CFT Law Article 16.1(c); AML-CFT Decision Articles 13.1, 14, 35.4, 38)

The Company is prohibited from the following activities:

- Establishing or maintaining any Customer or Business Relationship, conducting any financial or commercial transactions, keeping any Business Relationship under an anonymous or fictitious name or by pseudonym or number;
- Establishing or maintaining a Business Relationship or executing any business dealing in the event they are unable to complete adequate risk-based CDD measures in respect of the Customer for any reason;
- Dealing in any way with Shell Banks, whether to open accounts with the Company or to facilitate any banking transactions for themselves or on behalf of the customers;
- Invoking banking, professional or contractual secrecy as a pretext for refusing to perform statutory reporting obligation in regard to suspicious activity;
- Facilitating issuance of bearer shares or bearer share warrants.

13.5. MONEY LAUNDERING

(AML-CFT Law Articles 2.1-3, 4, 29.3, AML-CFT Decision Article 1)

The AML-CFT Law defines money laundering as engaging in any of the following acts wilfully, having knowledge that the funds are the proceeds of a felony or a misdemeanour (i.e., a predicate offence):

- Facilitating the transfer or movement of proceeds or conducting any transaction which results in concealing or disguising their Illegal source;
- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds;
- Acquiring, possessing or using proceeds upon receipt;
- Assisting the perpetrator of the predicate offense to escape punishment.

Money laundering is the process by which criminals attempt to hide or disguise the true origin and Ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. If carried out successfully, money laundering enables criminals to escape prosecution, maintain control over the proceeds of crime and continue their criminal activities.

The AML-CFT Law designates money laundering as a criminal offence. Its prosecution is independent of that of any predicate offence to which it is related or from which the proceeds are derived. The suspicion of money laundering is not dependent on proving that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved, but can be inferred from certain information, including indicators or behavioural patterns.

13.6. PREDICATE OFFENCES

The AML-CFT Law defines a predicate offence as “any act constituting an offence 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.” A predicate offence is therefore any crime, whether felony or misdemeanor, which is punishable in the UAE, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

FATF has designated 21 (twenty-one) categories of predicate offences, as follows:

- Participation in an organized criminal group and racketeering.
- Terrorism, including terrorist financing;
- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;

- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint and hostage-taking;
- Robbery or theft;
- Smuggling; (including in relation to customs and excise duties and taxes);
- Tax crimes (related to direct taxes and indirect taxes);
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.

Based on expert analysis of these categories conducted on behalf of the UAE's Competent Authorities for the 2018 National Risk Assessment, the top (highest) threats to the State in relation to money laundering have been identified as: fraud, counterfeiting and piracy of products, illicit trafficking in narcotic drugs and psychotropic substances, and professional third-party money laundering.

Similarly, other (medium-high) threats of particular concern to the UAE in relation to money laundering have been identified as the categories of: insider trading and market manipulation, robbery and theft, illicit trafficking in stolen and other goods, forgery, smuggling (including in relation to customs and excise duties and taxes), tax crimes (related to direct taxes and indirect taxes), and terrorism (including terrorist financing).

We are giving special attention to the most serious threats identified in the NRA and performing comprehensive Risk Assessment and Customer Due Diligence to verify the customer background before executing the customer onboarding and also the transaction.

13.7. TERRORISM FINANCING

An offense within the meaning of the UN International Convention for the Suppression of the Financing of Terrorism (1999), where a person by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

- An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex of the above-mentioned treaty, or

- Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing an act.

(AML-CFT Law Articles 3.1, 4, 29.3, AML-CFT Decision Article 1)

The AML-CFT Law designates the financing of terrorism as a criminal offence, which is not subject to the statute of limitations. It defines the financing of terrorism as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organization or terrorist person or intended to finance a terrorist organization, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or

- Providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or committing such acts on behalf of a terrorist organization or a terrorist person while aware of their true background or purpose.

In a 2019 report by MENAFATF, an assessment of the global threat posed by the financing of terrorism stated.

“The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organization’s such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfil their basic need to generate and manage funds is also evolving.

Terrorist organization’s use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation; and social services. These financial requirements are usually high for large terrorist organizations, particularly those that aim to, or do, control territory. In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management.”

13.8. FINANCING OF ILLEGAL ORGANISATIONS

(AML-CFT Law Articles 3.2, 4, 29.3, AML-CFT Decision Article 1)

The AML-CFT Law designates the financing of illegal organisations as a criminal offence that is not subject to the statute of limitations. The Law defines the financing of illegal organisations as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by an illegal organisation or by any person belonging to an illegal organisation or intended to finance such illegal organisation or any person belonging to it, even if without the intention to conceal or disguise their illicit origin.
- Providing, collecting, preparing, obtaining proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an Illegal organisation or of any of its members, with knowledge of its true identity or purpose.

When assessing the risk exposure to the financing of illegal organisations, the Company is placing significant emphasis on regulatory disclosure, accounting, financial reporting and audit requirements of organisations with which they conduct Business Relationships or transactions. This is particularly important where non-profit, community/social, or religious/cultural organisations are involved, especially when those organisations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason.

13.9. PROLIFERATION AND PROLIFERATION FINANCING

The threat posed by weapons of mass destruction (WMD) and their associated delivery systems is a distinct but related concept from the financing of such activity. Although the FATF has not presented official definitions of “proliferation” and “proliferation financing”, the FATF’s 2021 Guidance on Proliferation Financing Risk Assessment and Mitigation offers the following working definitions:

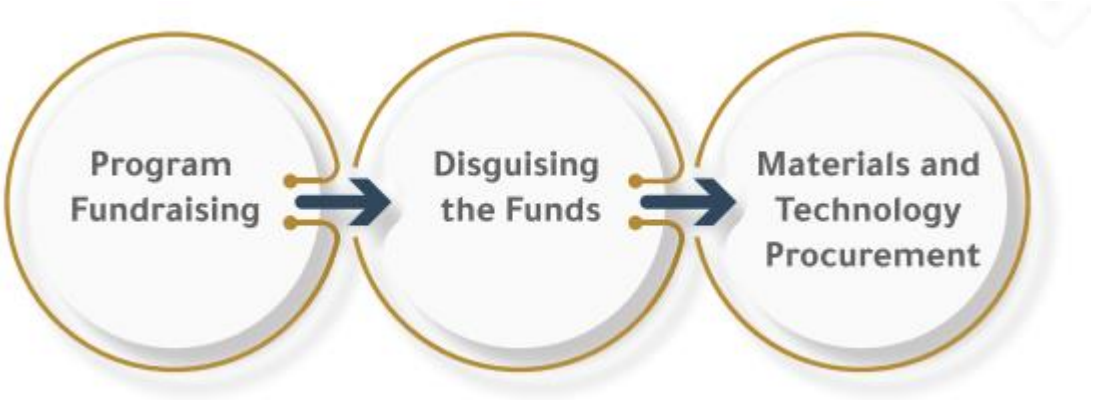
WMD Proliferation refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both Dual-Use technologies and Dual-Use goods used for non-legitimate purposes).

The Financing of Proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both Dual-Use technologies and Dual-Use goods for non-legitimate purposes).

Proliferation Financing Risk refers to the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in FATF Recommendation 7, namely those pursuant to UNSCRs relating to the prevention, suppression, and disruption of proliferation of WMD and its financing.

13.9.1. STAGES OF PROLIFERATION FINANCING

Proliferation Financing takes place over three stages:



Stage 1: Program Fundraising:

A proliferating country raises financial resources for in-country costs. The funding sources may derive from the proliferating country's budget, profits from an overseas commercial enterprise network, and/or proceeds from an overseas criminal activity network.

As an example of program fundraising, the UN Panel of Experts has found that North Korea/ DPRK has exported prohibited commodities (such as coal, iron and steel products, and copper) to generate revenue. International observers believe that the DPRK's sales of natural resources are part of elaborate trade-based payment schemes to support its WMD and conventional weapons program development.

Stage 2: Disguising the Funds:

The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes. A proliferating country may use means that range from the simpler to the more complex, including using normal correspondent banking channels or an intricate network of procurement agents and front companies. During this stage, states that are subject to comprehensive sanctions will seek to circumvent such sanctions, often using methods on the more sophisticated end of the spectrum to disguise the funds. Both Iran and the DPRK have been found to use front companies, shell companies, and complex, opaque ownership structures to evade and circumvent TFS.

Stage 3: Materials and Technology Procurement:

The proliferating state or its agents use the disguised resources for procurement of materials and technology within the international financial system. This stage also includes the payments for shipping and transport of materials and technology.

A past UN Panel of Experts report observed that Iran used various procurement methods, including using front companies for prohibited procurement, as well as using its petrochemical sector to obscure the end use of items procured for its nuclear program.

13.9.2. PROLIFERATION FINANCING THREATS, VULNERABILITIES, AND CONSEQUENCES

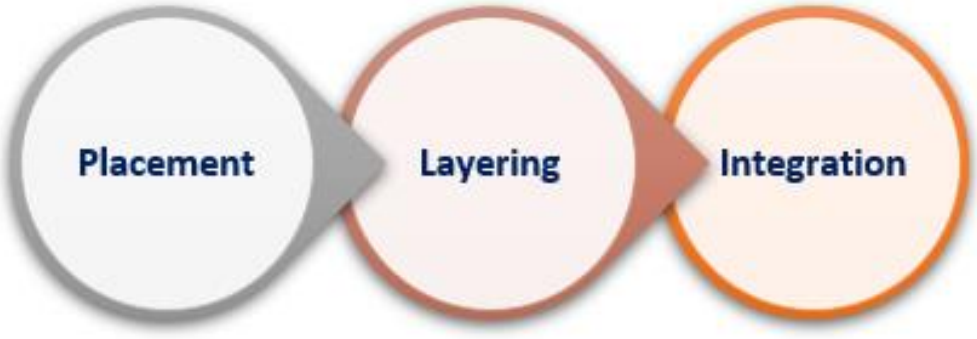
Threat refers to designated persons and entities that have previously caused or have the potential to evade, breach, or exploit a failure to implement TFS related to proliferation in the past, present, or future. Such threat may also be caused by those persons or entities acting for or on behalf of designated persons or entities.

Vulnerability refers to matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation, or evasion of TFS related to proliferation. Vulnerabilities may include features of a particular sector, a financial product, or type of service that make them attractive for a person or entity engaged in the breach, non-implementation, or evasion of TFS related to proliferation.

Consequence refers to the outcome where funds or assets are made available to designated persons and entities, which could ultimately allow them, for instance, to source the required materials, items, or systems for developing and maintaining illicit nuclear, chemical, or biological weapon systems (or their means of delivery), or where frozen assets of designated persons or entities would be used without authorisation for PF. A consequence may also include reputational damage. The ultimate consequence of PF is the use or threat of use of a WMD.

13.10. THE ML PHASES

The Company is fully aware of the three phases of money laundering. By determining for which ML/FT phase a certain product can be misused or the Company itself can be misused, will help the Company understand its specific inherent ML/FT risks. The paragraphs below describe the crime of money laundering as consisting of three distinct phases:



Placement.

In this phase, criminals attempt to introduce Funds or the Proceeds of Crime into the financial system using a variety of techniques or typologies.

Examples of placement transactions include the following:

- ✓ Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned businesses.
- ✓ Foreign exchange: Purchasing of foreign exchange with illegal funds.
- ✓ Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade attention or reporting requirements.
- ✓ Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- ✓ Loans: Repayment of legitimate loans using laundered cash.

Layering

Once the Funds or Proceeds are introduced, or placed, into the financial system, they can proceed to the next phase of the process; often, this is accomplished by placing the funds into circulation through formal financial institutions, and other legitimate businesses, both domestic and international. In this layering phase, criminals attempt to disguise the illicit nature of the Funds or Proceeds of Crime by engaging in transactions, or layers of transactions, which aim to conceal their origin.

Examples of layering transactions include:

- ✓ Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- ✓ Moving funds from one financial institution to another or within accounts at the same institution;
- ✓ Converting the cash placed into monetary instruments;
- ✓ Reselling high-value goods and prepaid access/stored value products;
- ✓ Investing in real estate and other legitimate businesses;
- ✓ Placing money in stocks, bonds or life insurance products; and
- ✓ Using shell companies to obscure the ultimate beneficial owner and assets.

Integration

In this phase, criminals attempt to return, or integrate, their “laundered” Funds or the Proceeds of Crime back into the economy, or to use it to commit new criminal offences, through transactions or activities that appear to be legitimate.

A key objective for criminals engaged in money laundering—and therefore a key generic risk underlying the specific risks faced by the Company—is the exploitation of situations and factors (including products, services, structures, transactions, and geographic locations) which favour anonymity and complexity, thereby facilitating a break in the "paper trail" and concealment of the illicit source of the Funds.

The Company is diligently ensuring that the business is not utilized, either directly or indirectly, to facilitate money laundering or the financing of terrorism or illegal organisations in any of the three stages.

13.11. ML/FT TYPOLOGIES

The methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organisations are continually evolving and becoming more sophisticated. Moreover, the variety of transaction and activity types involving DPMS can be very wide. It is therefore impossible to provide an exhaustive list of ML/FT typologies for DPMS, as new typologies and techniques are constantly being developed and attempted.

Nevertheless, research on the subject and analysis of case studies from around the world have identified some common methods used by criminals for the purposes of ML/FT involving DPMS. These methods broadly align with the classical stages of the ML/FT process i.e. placement, layering, and integration; however, they can also involve PMS as a vehicle for committing a predicate offence, or as the direct proceeds of crime

The following have been identified as being amongst the common typologies used for exploiting DPMS for the purpose of ML/FT, according to the Financial Action Task Force (FATF):

- Use of PMS as an alternative to currency.
- PMS as stored value instruments/means to realize the proceeds of crime
- Laundering illegal PMS and/or the use of PMS to launder the proceeds of crime.
- Trade-based ML.
- Physical smuggling of PMS.

13.12. SANCTIONS AGAINST PERSONS VIOLATING REPORTING OBLIGATIONS

(AML-CFT Law Articles 15, 24, 25)

The AML-CFT Law provides for the following sanctions against the Company, managers or employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering or the financing of terrorism or of illegal organisations:

- ✓ Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- ✓ Any of these two sanctions.

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a Crime. It should also be noted that the transactions or funds that are the subject of the suspicion may represent only part of the proceeds of the criminal offence, regardless of their value Likewise, the AML-CFT Law provides for sanctions against anyone who warns or notifies a person of a suspicious transaction report or reveals that a transaction is under review or investigation by the Competent Authorities, as follows:

- ✓ Imprisonment for no less than six months and a penalty of no less than AED100,000 and no more than AED 500,000; or
- ✓ Any of these two sanctions.

Part - II

IDENTIFICATION AND ASSESSMENT OF ML/TF RISKS

14. IDENTIFICATION AND ASSESSMENT OF ML/TF RISKS

(AML-CFT Law Article 16.1; AML-CFT Decision Article 4.1)

Both the AML-CFT Law and the AML-CFT Decision provide that the Company utilize a risk-based approach with respect to the identification and assessment of ML/FT risks. The Company is obliged to assess and to understand the ML/FT risks to which they are exposed, and how they may be affected by those risks. Specifically, the AML-CFT Law provides that the Company:

"…continuously assess, document, and update such assessment based on the various risk factors established in the Implementing Regulation of this Decree-Law and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority upon request."

Additionally, the Company is entrusted with the responsibility, as per AML-CFT Decision, to fulfil the following charges:

"…Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."

14.1 RISK-BASED APPROACH

A risk-based approach (RBA) is central to the effective implementation of the AML/CFT legislation. The RBA helps the Company to identify and assess the risks associated with their clients and transactions and take appropriate measures to mitigate those risks. The Company has implemented the appropriate systems and controls to address the risks of money laundering and terrorist financing. Assessing these risks and creating a good AML/CFT compliance program, the Company can optimize the use of their resources more efficiently and effectively within the scope of the national AML/CFT legislative and regulatory framework. and ensuring compliance with the AML/CFT legal and regulatory requirements. The Company can consider its own nature, size, and complexity when designing its anti-money laundering (AML) and counter-terrorist financing (CTF) systems and controls.

14.2 RISK ASSESSMENT: NATIONAL (NRA)

A decision taken by the UAE National Committee for Anti-Money Laundering and Combating the Financing of Terrorism No. (214) of 2017 issued on 29/05/2017 (update to Resolution No. 149 of 2016 issued on 12/06/2016) regarding the formation of the Sub-Committee for the National Risk Assessment for Money Laundering and Financing of Terrorism Risks in the United Arab Emirates (hereinafter referred to as the NRA Sub-committee) started the process of developing the NRA for ML and TF risks in the UAE, which had not been conducted previously.

This initial NRA assessment is a FATF requirement, and a first step in the Mutual Evaluation process to implement FATF and MENAFATF recommendations after their assessment of the UAE in 2019-2020.

The NRA has helped the UAE and its public and private sector partners to have a more comprehensive and shared understanding of the inherent ML/TF risks facing the nation as a whole (i.e., risks prior to the application of numerous mitigations and controls). The NRA also provides a basis on which to formulate appropriate policies and activities to mitigate the impact of the inherent risks identified. The FATF assessment of effectiveness of the UAE's AML/CFT efforts will always refer back to the threats, vulnerabilities and risks identified in the NRA.

14.3 RISK FACTORS

(AML-CFT Law 16.1(a)-(b); AML-CFT Decision 4.1(a))

Proper identification of risk factors is crucial to the effective implementation of a risk-based approach to assessing and mitigating ML/FT risk. Identified risk factors are used for the accurate categorisation of risks, as well as for the application of appropriate mitigation measures at both the enterprise and the customer level. At the enterprise level, this includes adopting and applying adequate policies, procedures, and controls to business processes. At the customer level, this includes assigning appropriate risk classifications to customers and applying due diligence measures that are commensurate with the identified risks.

The AML-CFT Decision outlines several risk factors, the Company is actively evaluating and analyzing its exposure to money laundering and financing of terrorism risks when identifying and assessing the ML/FT risk exposure. The Company is considering a wide array of additional risk factors, utilising risk identification methods or combinations of methods that are appropriate to the particular circumstances.

Examples of such methods include, but are not limited to:

- Checklists of ML/FT red-flag indicators;
- Input and information from relevant internal sources, including the designated AML/CFT compliance officer;
- Information from national sources, including the results of the NRA with regard to ML/FT trends and sectoral threats and notices or circulars from the relevant Supervisory Authorities;
- Information from publications of relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, UNODC, and others.

14.4 OUR OWN ML/TF RISK IDENTIFICATION AND ASSESSMENT

The Company implemented the risk assessment procedures based on the NRA – National Risk Assessment guidance and Identification and Assessment of ML/FT Risks and Mitigation of ML/FT Risks from the Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions March 2021.

The company is using LiveEx Shield for the risk assessment process in accordance with the following procedure:

- ✓ Identifying inherent risks
- ✓ Assessing of the Inherent Risks
- ✓ Design an action Plan
- ✓ Implement the action Plan
- ✓ Assessing residual risks

This ML/TF risk assessment methodology defines each risk dimension used in the organization ML/TF risk assessment, considering the following dimensions of ML/TF risk:

Customer Risk;

Counterparty/customer type, complexity and transparency (e.g. whether the counterparty or customer is a natural 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 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;

Jurisdictional Risk or Country Risk;

Country of origin of the PMS—particularly in relation to whether the country is a known production or trading hub for the type of PMS; has adequate regulations and controls (for example, is a participant in the 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 organisations);

Counterparty Risk;

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—see Guidelines Section 6.4.3)—particularly in relation to the locations where the transaction is conducted and the goods are delivered;

Delivery 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);

Product Risk;

Type, nature and characteristics of the products and/or services, including but not limited to: quantity, quality/level of purity, price/value, form (whether physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity;

Transaction Related Risk;

Type, size, complexity, cost and transparency of both the transaction (including whether the physical or virtual exchange of merchandise is involved) and the means of payment or financing—particularly in relation to whether they appear to be consistent with the counterparty or customer's socio-economic profile (see Guidelines Section 4.4.3, among others), local market practices, and the degree of expertise required;

Other Risks;

Novelty or unusual nature of the transaction or financial arrangements (including, for example, requirements to expedite the transaction beyond what is customary, unusual delivery requirements, or unusual requests for secrecy), particularly compared with what is normal practice in the local market

The above risk types are segregated into detailed risk factors to assess and determine the level of ML/TF risk for the Company. The assessment performed in a holistic manner.

The Company's compliance committee has identified the customer risk based on the following parameters;

Risk Category	Action Required	Risk Controls
Low	CDD – Customer Due Diligence	Customer Identity Documents Collection and Sanction Screening verification.
Medium	EDD – Enhanced Customer Due Diligence	Customer Identity Documents Collection, Sanction Screening Verification, Customer Risk Assessment and Transaction Purpose
High	EDD – Enhanced Customer Due Diligence & Ongoing Monitoring	Customer Identity Documents Collection, Sanction Screening Verification, Customer Risk Assessment, Transaction Purpose, Source of Fund and documents support (i.e., BLs, Invoices, Transport Docs).

Part - III

MITIGATION OF ML/TF RISKS

15. ELEMENTS OF AN AML/CFT PROGRAM

The three lines of defense are the basic elements of the Company's AML/CFT Program.

First line of defense - A system of internal policies, procedures and controls, including an ongoing AML/CFT & TFS employee training program

Second line of defense - A designated compliance officer or money laundering reporting officer

Third line of defense - An independent audit function to test the overall effectiveness of the AML program

16. INTERNAL POLICIES, CONTROLS AND PROCEDURES

An effective AML program requires a comprehensive set of policies, procedures, and internal controls that are tailored to the company's specific risks and business activities. It involves ongoing monitoring and testing to ensure that it is effective and responsive to changes in the regulatory environment and the Company's risk profile. An effective AML program is critical for mitigating the risk of financial crimes and ensuring compliance with applicable laws and regulations.

AML Policy:

The Company's AML policy is a written statement that outlines the company's commitment to comply with AML laws and regulations and this policy reflects the Company's risk profile, business activities, and regulatory requirements. It includes procedures for identifying and verifying customer identities, monitoring transactions, and reporting suspicious activities and also provide guidance on employee training and reporting requirements.

AML Procedures:

The Company's AML procedures provides detailed guidance on how to implement the AML policy effectively and it is practical, easy to follow, and tailored to the Company's specific risks and business activities. AML procedures covers all relevant AML activities, including customer due diligence, transaction monitoring, and suspicious activity reporting. The procedures are regularly reviewed and updated to reflect changes in the regulatory environment and the Company's risk profile.

Internal Controls:

The Company's internal controls are the processes and procedures that help the Company to manage risks and active its objectives. These controls are designed to prevent money laundering activities, detect potential AML risks and ensure compliance with relevant laws and regulations. Effective AML internal controls may include KYC procedures, CDD processes, transaction monitoring, and SAR reporting. The internal controls are regularly monitored and tested to ensure

that they are effective and responsive to changes in the regulatory environment and the Company's risk profile.

The Company designed the internal policies, controls and procedures to prevent, detect and deter ML/FT risks can be categorized broadly as those related to:

- ✓ The identification and assessment of ML/FT risks
- ✓ Customer due diligence (CDD), including enhance due diligence (EDD), and simplified due diligence (SDD), including its review and updating, and reliance on third parties in regard to it.
- ✓ Customer and transaction monitoring, and the reporting of suspicious transactions
- ✓ AML/CFT governance, including compliance staffing and training, senior management responsibilities, and the independent auditing of risk mitigation measures.
- ✓ Record-keeping requirements.

17. CUSTOMER DUE DILIGENCE (CDD)

Customer due diligence is a term that refers to the process of verifying the identity of a customer, assessing the risks associated with that customer, and ensuring that their activities are in compliance with legal and regulatory requirements.

Main elements of a customer due diligence program

- ✓ Customer Identification;
- ✓ Profiles;
- ✓ Customer Acceptance;
- ✓ Risk rating;
- ✓ Monitoring;
- ✓ Investigation; and
- ✓ Documentation

17.1 RISK-BASED APPLICATION OF CDD MEASURES

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

- ➢ Identification of the customer, Beneficial Owners, beneficiaries, and controlling persons; and the verification of their identity on the basis of documents, data or information from reliable and independent sources
- ➢ Screening of the customer, Beneficial Owners, beneficiaries, and controlling persons, to screen for the applicability of targeted or other international financial sanctions, and,

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

- Obtaining an understanding of the intended purpose and nature of the Business Relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure
- Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behaviors.
- Scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the customer, their business and risk profile, including where necessary, the source of funds
- Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

As part of their overall AML/CFT framework, the Company developed the internal CDD policies, procedures and controls. Considerations to make include the following:

- The outcomes of the ML/TF business risk assessment;
- Circumstances, timing, and composition in regard to the application of CDD measures;
- Frequency of reviews and updates in relation to CDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which CDD measures are applied.

17.2 CUSTOMER AND BENEFICIAL OWNER IDENTIFICATION AND VERIFICATION

(AML-CFT Decision Articles 4.2(b), 3(a), 5.1, 8.1, 9, 10, 11.2, 13.1, 14.2)

Based on the principles of "Know Your Customer" and risk-based CDD, the identification and verification of the identity of customers is a fundamental component of an effective ML/FT risk management and mitigation programme. In accordance with Cabinet Resolution No. 58 of 2020 regulating the Beneficial Owner Procedures (the UBO Resolution), The Company is obliged to identify customers, including the Beneficial Owners, beneficiaries, and controlling persons, whether permanent or walk-in, and whether a natural or legal person or Legal Arrangement, and to verify their identity using documents, data or information obtained from reliable and independent sources.

The core components of a customer's identification are;

Personal data, including details such as the name, passport or identity card number, country of issuance, date issuance and expiry date of the identity card or passport, nationality, date and place of birth (or date and place of establishment or incorporation, in the case of a legal person or arrangement); and

Principal address, including evidence of the permanent residential address of a natural person, or the registered address of a legal person or arrangement.

With regard to the identification and verification of the identity of foreign nationals, whether customers or Beneficial Owners, beneficiaries or controlling persons, The Company take steps to understand and request only those types of identification documents that are legally valid in the relevant jurisdictions. Furthermore, when verifying the identity of foreign nationals associated with high-risk factors, we should validate the authenticity of customer identification documents obtained.

The types of address verification that may generally be considered acceptable include, but are not limited to, the following categories of documents issued in the name of the customer:

- Bills or account statements from public utilities, including electricity, water, gas, or telephone line providers;
- Local and national government-issued documents, including municipal tax records;
- Registered property purchase, lease or rental agreements;
- Documents such as bank statements, credit or debit card statements, or insurance policies.

In relation to legal persons and legal arrangements:

- We identify and verify the identity of customers, Beneficial Owners, beneficiaries, and controlling persons, and verify the identity of any person legally empowered to act or transact business on behalf of the customer, whether the customer is a legal or natural person. Such persons may include:
  - Signatories or other authorized persons in case they are authorized to act on behalf of the customer;
  - Parents or legal guardians of a minor child, or legal guardians of a physically or mentally disabled or incapacitated person;
  - Attorneys or other legal representatives, including liquidators or official receivers of a legal person or arrangement.

In the event that a legally empowered representative is also a legal person or Legal Arrangement, the normal CDD procedures for such entities should be applied.

- When verifying that a person purporting to act on behalf of a customer is so authorised, the following types of documents may generally be considered to be acceptable
  - A legally valid power-of-attorney;
  - A properly executed resolution of a legal person's or Legal Arrangement's governing board or committee;
  - A document from an official registry or other official source, evidencing ownership or the person's status as an authorised legal representative;
  - A court order or other official decision.

18. ENHANCED DUE DILIGENCE

Enhanced Due Diligence is an important component of an effective anti-money laundering and counter-terrorism financing program, as it can help prevent organizations from becoming unwittingly involved in illegal activities.

Enhanced due diligence (EDD) refers to a more extensive and rigorous process of investigating and verifying the identity, background, and financial status of a client or business partner, usually in the context of anti-money laundering (AML) and counter-terrorism financing (CTF) measures.

Enhanced due diligence implies an increased level of scrutiny and investigation beyond the standard due diligence procedures. It may involve additional measures such as verifying the source of funds, conducting interviews with key stakeholders, reviewing past transactions and legal history, and checking for any potential risks or red flags.

18.1 EDD FOR LEGAL ENTITY / CORPORATE CUSTOMER

Relationship with a business entity such as a company is obtaining and verifying suitable documents in support of name, address and business activity – such as a copy of a business registration, a certificate of incorporation, a memorandum of association, articles of association, passport copies of the directors and shareholders, proof of address, or beneficial owner verification.

The Company is obtaining the details of all employees who would be authorized to transact on behalf of the company, or firm and documents of their identification, together with their signatures. Copies of all documents called for verification should be kept on record.

The controls built in the system ensure that customer and UBO information is mandatory to obtain while processing a transaction. This is a vital preventive approach that supports in effectively filtering suspicious activity in a proactive manner, and in compliance with regulatory requirements.

Legal Entity/Corporate Customer Onboarding Process

The following details are required for legal entities;

- Legal Entity information (Company details, directors, beneficial owner, etc.)
- Identification records (trade license, ID proofs of UBO)
- Other required documents (MOA, AOA, certificate of Incorporation, audited financials, bank statements etc.)
- Customer profile / KYC Form
- VAT Registration Certificate
- Proof of Address -Latest Telephone/Electricity bill copy/Tenancy copy

Verification

- Confirmation about the physical appearance (business address)
- Business Activities is aligned with Trade License or not
- Verifying Telephone Number and Email ID

Compliance Approval

If the customer profile or any one of the parties matched with the following lists, the system will automatically escalate the profile to compliance officer approval.

- UAE Local Terrorist List
- UNSC Consolidated List
- Internal Watch List

19. ENHANCED DUE DILIGENCE FOR HIGH-RISK CUSTOMERS OR TRANSACTIONS

The AML-CFT Decision defines a High-Risk Customers as including those who represent 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 customer 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..."

High-Risk Classification:

- The level of complexity and transparency of the customer's transactions, especially in comparison with the customer's or Beneficial Owner's educational and professional background.
- The level of complexity and transparency of the customer's legal structure of legal persons or arrangements.
- The nature of any other business interests of the customer or Beneficial Owner, including any other legal persons or arrangements owned or controlled.
- Consistency between the customer's line of business and that of the counterparty to the customer's transactions (as identified, for example, through internet searches).

The Company is obliged to collect the following documents / additional information / evidence from high-risk customers such as:

- Source of wealth;
- Banking references;

- 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.

20. REQUIREMENTS FOR HIGH-RISK COUNTRIES

The Company adopts Enhanced Due Diligence (EDD) measures that align with the Money Laundering (ML) and Financing of Terrorism (FT) risks related to Business Relationships and transactions involving customers from high-risk countries, which are subject to a Call for Action and Jurisdictions under Increased Monitoring, as well as the countries identified by NAMLCFTFC. Similarly, for legal persons and arrangements, the Company applies EDD to the Beneficial Owners, beneficiaries, and other controlling persons from high-risk countries.

The Company seeks guidance on high-risk countries from various sources, including NAMLCFTFC, the FATF list of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring, and NRA reports. Additionally, the Company refers to the Organisation for Economic Cooperation and Development (OECD) list of jurisdictions classified as tax havens. The Basel AML index also serve as a valuable resource to assess the risk associated with a country.

Examples of some of the measures the Company applies in this regard include:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;
- 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 the purpose of individual transactions;
- Increased investigation to ascertain whether the customers or related persons (Beneficial Owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPs;
- Increased supervision of the Business Relationship, including the requirement for higher levels of internal reporting and senior management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information.

Additionally, the Company implements all specific CDD measures and countermeasures regarding High-Risk Countries as defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, including those related to the implementation of the decisions of the UN Security Council under Chapter VII of the Charter of the United Nations, the International Convention for the Suppression of the Financing of Terrorism and the Treaty on the Non-Proliferation of Nuclear Weapons, and other related directives, and those called for by the Financial Action Task Force (FATF) and/or other FSRBs.

As part of the overall AML/CFT framework, we developed risk-based internal policies, procedures and controls in connection with the application of EDD measures.

Examples of the some of the factors they should consider when developing the risk-based policies include:

- the ML/FT risks identified in the ML/TF business risk assessment;
- Circumstances, timing, and composition regarding the application of EDD measures;
- Frequency of reviews and updates in relation to information on high-risk customers;
- Extent and frequency of ongoing monitoring of the Business Relationship and monitoring of transactions in relation to high-risk customers.

21. EDD FOR POLITICALLY EXPOSED PERSONS (PEPs)

The AML-CFT Law and the AML-CFT Decision define PEPs as:

"Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of 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 organisation or any prominent function within such an organisation; and the definition also includes the following:

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

  - Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP.
  - Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.

The Company is also required to take reasonable measures to establish the source of funds and the source of wealth of customers and Beneficial Owners identified as PEPs. In this regard, and commensurate with the nature and size of their businesses, DNFBPs should take measures that include:

- 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.

If a customer, Beneficial Owner, beneficiary, or controlling person is identified as a PEP, the Company is taking reasonable measures to establish the PEP's source of funds and source of wealth and evaluating the legitimacy of the source of funds and source of wealth, including making reasonable investigations into the individual's professional and financial background.

The Company is obtaining senior management approval before establishing a Business Relationship with a PEP, or before continuing an existing one. In regard to the latter, senior management should be notified and their approval should be obtained for the continuance of a PEP relationship each time any of the following situations occur:

- An existing customer, Beneficial Owner, beneficiary, or controlling person becomes, or is newly identified as, a PEP;
- An existing PEP Business Relationship is reviewed and the CDD information is updated, either on a periodic or an interim basis, according to the Company's internal policies and procedures;
- A material transaction that appears unusual or illogical for the PEP Business Relationship is identified.

22. HIGH-RISK JURISDICTIONS

As per the Circular No: MOEC/AML/004/2024 on updating the list of High-Risk Countries. Reference to article 12 of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering, and Combating the Financing of Terrorism and the Financing of illegal organizations and its amendments regarding the competences of National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations, and with reference to Article 22 of the 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 the Financing of illegal organizations and its amendments, the Company has established robust protocols to ensure compliance with international regulations, including those concerning Designated Non-Financial Businesses and Professions (DNFBPs) and jurisdictions on the Blacklist.

As per our internal policy that we will not engage in any business relationships or transactions with entities or individuals operating within jurisdictions that have been blacklisted. We are committed to upholding the integrity of our operations and safeguarding against any potential risks associated with such dealings.

If we become aware that any of our suppliers or customers are engaged in activities outlined in the jurisdictions on the Blacklist, we will terminate the business relationships with the non-compliant parties and blocking any further transactions or dealings with them. Additionally, we will promptly report such occurrences to the competent authorities, ensuring that appropriate measures are taken to address the situation in accordance with regulatory guidelines.

By proactively taking these steps, we affirm our unwavering commitment to compliance and underscore our dedication to conducting business with the utmost integrity and accountability. These measures are vital to protecting our operations and upholding the trust and confidence of our stakeholders.

23. JURISDICTIONS UNDER INCREASED MONITORING

As per the Circular No: MOEC/AML/004/2024 on updating the list of High-Risk Countries. Reference to article 12 of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering, and Combating the Financing of Terrorism and the Financing of illegal organizations and its amendments regarding the competences of National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations, and with reference to Article 22 of the 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 the Financing of illegal organizations and its amendments, the Company is committed to adhering to the highest standards of compliance, particularly concerning the identification and mitigation of risks associated with jurisdictions listed on the Grey List.

To ensure robust compliance measures, we have implemented a comprehensive risk-based approach to customer due diligence. This approach involves thorough customer and beneficial owner identification and verification procedures for both natural and legal persons. We are conducting ongoing monitoring and regularly review and update customer due diligence information to reflect any changes in risk profiles.

High risks are identified, such as transactions or customers involving high-risk countries, we apply enhanced due diligence measures.

By consistently applying risk-based customer due diligence measures, we maintain string compliance culture to mitigate financial crime risks. These measures ensure that our operations are safeguarded against potential threats to both our business and the wider financial system.

24. SIMPLIFIED DUE DILIGENCE (SDD) MEASURES

(AML-CFT Decision 4.3, 5, 10)

The Company is only permitted to exercise simplified customer due diligence measures (SDD) with regard to customers identified as low-risk through an adequate analysis of risks and in the absence of a ML\FT suspicion.

SDD generally involves a more lenient application of certain aspects of CDD measures, including elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification;
- Fewer and less detailed inquiries in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- More limited supervision of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

As part of their overall AML/CFT framework, the Company use a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of SDD procedures. Examples of some of the factors they should consider when developing their risk-based policies include:

- the ML/FT risks identified in the ML/TF business risk assessment, especially with regard to low-risk categories of customers;
- Circumstances, timing, and composition in regard to the application of SDD measures;
- Frequency of reviews and updates in relation to customer SDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which SDD measures are applied.

25. SANCTION SCREENING

Sanction screening is an essential component of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) compliance programs. Sanction screening refers to the process of searching and verifying the identities of individuals and entities against the UAE Local Terrorist List and UN Consolidated List using advanced screening technology. Sanction screening involves collecting and verifying customer data, such as name, date of birth, and address, and comparing it to UAE Local Terrorist List and UN Consolidated List. This process can be automated, which allows for real-time screening of individuals and entities during account opening, transaction processing, and other key business activities.

As per Article 21.2 of Cabinet Decision 74, Dealers in Precious Metal Stones (DPMS) are required to perform regular searches against applicable sanctions lists of their customer databases, parties to any transactions, potential customers, beneficial owners, and persons and organizations with which the company has a direct or indirect relationship, as well as continuous searches of the customer database before conducting any transaction or entering into a business relationship with any person. Sanctions screening systems and processes are essential, but are also only as effective as the customer and transactional information used when comparing against applicable sanctions lists. Therefore, effectiveness depends critically on the completeness and accuracy of information obtained through the application of CDD/KYC measures and contained in payment instructions and other transactional data fields.

An effective sanctions screening program consists of the following core elements:

- A well-calibrated risk-based framework
- Robust training and risk awareness
- Meaningful integration into the sanctions program
- Active oversight

25.1 OVERVIEW OF NAME SCREENING

As per the Executive Office's Guidance on TFS for Designated Non-financial Business and Professions, name screening (whether automated or manual) must be performed prior to the onboarding of a customer and/or the facilitation of an occasional transaction and on an ongoing basis. As indicated above, name screening encompasses any data set within the Company operations, separate from its transaction records, that may present a relevant sanctions risk indicator or be conducive to detection through screening on a periodic basis and prior to entering into a customer relationship.

Data relevant for name screening may include:

Customer data, including the names and addresses of existing or prospective customers, their beneficial owners, and other related or connected parties whose information is collected pursuant to risk-based due diligence procedures;

Employee data, including employee names and addresses; and

Third-party service provider data, including the names, addresses, and beneficial owners of an DPMS vendors, landlords, and tenants, as applicable.

Not all data elements within the Company records are relevant for sanctions screening. When determining what reference data should be screened, the Company should identify the data within its operations and records that is relevant to sanctions risk, determine how it is relevant, ensure it is conducive to effective screening, and differentiate it from data that is not relevant or suitable to screening. For example, the names of individuals and entities with whom the DPMS has a relationship are relevant for screening against name-based sanctions lists but not for geographic (region- or country-based) sanctions programs. Likewise, while the data contained in the addresses of such individuals and entities may not be directly relevant for screening against name-based sanctions lists, this data may assist in differentiating a true name match from a false name match when reviewing apparent name screening hits.

The Company also define other data elements (such as date of birth, nationality, and place of birth) that may be relevant for sanctions screening in some situations but not others. Date of birth, for example, is relevant as a distinguishing factor to assess a potential or a true match from a false match on an individual and might be used for screening in combination with another attribute, such as a name. In each case, the Company should weigh up the relative incremental value of screening the data element against the reliability of the data and whether an alert against the data will meaningfully assist in detecting or preventing a sanctions risk that would not be reasonably detected through other controls, or by screening different data attributes.

The screening criteria used by the Company to identify name variations and misspellings should be based on the level of sanctions risk associated with the particular product or type of transaction.

25.2 OVERVIEW OF TRANSACTION SCREENING

The Company screens all payments prior to completing the transaction (also referred to as "real-time" screening), utilizing all transaction records necessary to the movement of value between

parties and at a point in the transaction where detection of a sanctions risk is actionable to prevent a violation. The Company should then identify which attributes within those records are relevant for sanctions screening and the context in which they become relevant. As with name screening, names of parties involved in a transaction are relevant for list-based sanctions programs, whereas addresses are more relevant to screening against geographic sanctions programs but can be used as identifying information to help distinguish a potential or true match from a false match under a list-based program.

Data relevant for transaction screening may include:

- The parties who are all involved in a transaction;
- Agents, suppliers, and intermediaries involved in a transaction;
- Bank names, Bank Identifier Codes ("BICs"), and other routing codes.

Transaction screening is performed at a point in time where a transaction can be stopped and before a potential violation occurs. This typically occurs at a number of points in the lifecycle of a transaction, but certainly prior to executing any commitment to move funds. Particular attention directed to any points within the transactional process where relevant information could be changed, modified, or removed in order to undermine screening controls.

The Company is using LiveEx Shield software is configured to execute a real – time name screening on every customer, beneficiary / beneficial owner / partner's /shareholders, representatives, and all parties involved in the transaction activity. Every customer onboarding and Transaction will be screened related to blacklisted or sanctioned entities. Therefore, when a generated alert is investigated, the Compliance Officer / MLRO considers the following variables in order to identify possible matches:

a) Full Name

b) Nationality

c) Date of Birth

d) Place of Birth

Sanctions & PEP screening refers to the process of screening customer details against the different lists of sanctions for PEP status and whether the customer is involved in money laundering or terrorist activities. The customer details are screened in the following list:

- UNSC: United Nations Security Council Consolidated List;
- UAE - Local Terrorist List
- OFAC: Office of Foreign Assets Control - Specially Designated Nationals List (SDN)
- OFAC: Office of Foreign Assets Control - Consolidated Sanctions List;
- EU: European Union Consolidated list;
- Dow Jones; and
- Internal Watch List.

The Company takes all required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices.

We are conducting EDD on all PEPs / FPEPs / HIOs / PEP Associates / Diplomatic Passport Holders, whether natural person customers or the UBOs of legal persons or legal arrangements. Upon establishing a relationship with the customer, we ensure that that the customer undergoes review checks and verification at least on an annual basis or prior to carrying out the first transaction following the expiration of the 12-month period.

Part - IV

ADMINISTRATION AND REPORTING

26. SUSPICIOUS TRANSACTION REPORTING

(AML-CFT Law Articles 9.1, 15, 30; AML-CFT Decision Articles 16-18)

The AML/CFT legal and regulatory framework of the UAE, the Company is obliged to promptly report to the Financial Intelligence Unit (FIU) suspicious transactions and any additional information required in relation to them, when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime. The Company is required to put in place and update indicators that can be used to identify possible suspicious transactions.

Any suspicious transactions or activities that might be related to sanctions evasion, and which do not include confirmed or partial name matches to the UAE Local Terrorist List or UN Consolidated List, reported to the FIU by raising a STR/SAR through the goAML platform. In the context of implementing TFS, the Company is to familiarize with the TFS-related Reasons for Reporting (RFRs) in goAML. Below is a non-comprehensive list of TFS related RFRs when raising STRs/SARs:

- Customer is engaging in complex commercial deals and arrangements that seem to be aiming to hide the final destiny of the transaction/good or the beneficial owner, which could be a designated individual, entity, or group. (E.G: the use of a front company, middlemen, or intermediaries by the designated individual to circumvent the targeted financial sanctions).
- Customer is carrying out multiple ATM cash withdrawals in short succession across various locations in territories where sanctioned people have influence or around the border of sanctioned countries linked to terrorist financing.
- Customer is suspected to be working or acting on behalf of, or is controlled by, a sanctioned individual, entity, or group.
- Customer or transaction is suspected of being linked (directly or indirectly) to DPRK's nuclear-related, WMD-related, or ballistic missiles weapons program.
- Customer or transaction is suspected of being linked (directly or indirectly) to IRAN's nuclear weapons program.
- Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.
- Transaction involves sale, shipment, or export of dual use goods incompatible with the technical level of the country to which it is being shipped.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Inclusion of the individual/entity in the international sanctions list e.g. OFAC, UKHMT, EU, etc.

The Company implemented adequate internal policies, procedures and controls in relation to the identification and the immediate reporting of suspicious transactions.

26.1. ROLE OF THE FINANCIAL INTELLIGENCE UNIT

(AML-CFT Law Articles 9-10; AML-CFT Decision Articles 13, 16, 17.1, 21.2 and 5, 40- 43, 46.1-4, 49.2-3)

The FIU of the UAE is established within the premises of the Central Bank, however, the FIU operates independently by legal and regulatory mandate as the central national agency with sole responsibility for performing the following functions:

- ✓ Receiving and analysing STRs from the Company, and disseminating the results of its analysis to the Competent Authorities of the State;
- ✓ Receiving and analysing reports of suspicious cases from the Federal Customs Authority;
- ✓ Requesting additional information and documents relating to STRs, or any other data or information it deems necessary to perform its duties, from the Company, and Competent Authorities, including information relating to customs disclosures;
- ✓ Cooperating and coordinating with Supervisory Authorities by disseminating the outcomes of its analysis, specifically with respect to the quality of STRs, to ensure the compliance of the Company with their statutory AML/CFT obligations;
- ✓ Sending data relating to STRs and the outcomes of its analyses and other relevant data, including information obtained from foreign FIUs, to national Law Enforcement Authorities, prosecutorial authorities and judiciary authorities when actions are required by those authorities in relation to a suspected crime
- ✓ Exchanging information with its counterparts in other countries, with respect to STRs or any other information to which it has access.

Under the aegis of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, and for the effective performance of its functions, the FIU maintains operational protocols with numerous national and international Competent Authorities.

The FIU has launched the GoAML system for the purposes of facilitating the filing of STRs by all the Company. The Company is registered in the GoAML system by following the procedure manual and maintain their registration in an active status. GoAML provides a secure link of the Company to the FIU through their respective supervisory authorities. The system hosts processes for facilitating filing of STRs. The guidance documents for filing of STRs are posted on the dashboard of this system.

The STRs are received by the FIU and processed for any required further information or documents or for further action by Law Enforcement or Supervisory Authorities. The FIU maintains a record of these STRs, performs a trend analysis to understand the prevailing trends in transactions and sectors or Institutions where possibility of ML or FT exists and this trend analysis is shared with all the registered users of GoAML through the system by means of a periodic trends and typologies report.

26.2. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

(AML-CFT Decision 16)

The Company is obliged to put in place indicators that can be used to identify suspicious transactions, and to update those indicators on an ongoing basis in accordance with the instructions of the Supervisory Authorities or the FIU, as well as in keeping with relevant developments concerning ML/FT typologies. The Company also consider the results of the NRA, any Topical Risk Assessment and their own ML/FT business risk assessments in this regard.

As part of their overall AML/CFT framework, and commensurate with the nature and size of their businesses, the Company determine the internal policies, procedures and controls, apply in connection with the identification, implementation, and updating of indicators, as well as with the identification and evaluation of potentially suspicious transactions. Some factors that should be considered include, but are not limited to:

- Organisational roles and responsibilities with respect to the implementation and review/updating of the relevant indicators, especially in relation to obligatory indicators quired by the Supervisory Authorities or the FIU;
- Operational and IT systems procedures and controls in connection with the application of relevant indicators to processes such as transaction handling and monitoring, customer due diligence measures and review, and alert escalation;
- Staff training in relation to the identification and reporting of suspicious transactions (including attempted transactions), the appropriate use and assessment of the relevant indicators, and the degree and extent of internal investigation that is appropriate prior to the reporting of a suspicious transaction.

A few examples of potentially suspicious transaction types that the Company should take into consideration include:

- Transactions or series of transactions that appear to be unnecessarily complex, that make it difficult to identify the Beneficial Owner, or that do not appear to have an economic or commercial rationale;
- Numbers, sizes, or types of transactions that appear to be inconsistent with the customer's expected activity and/or previous activity;
- Transactions that appear to be exceptionally large in relation to a customer's declared income or turnover;
- Large unexplained cash amounts, especially when they are inconsistent with the nature of the customer's business;
- Loan repayments that appear to be inconsistent with a customer's declared income or turnover;
- Early repayment of a loan followed by an application for another loan;
- Third-party loan agreements, especially when there are amendments to or assignments of the loan agreement;
- Requests for third-party payments, including those involving transactions related to loans, investments, or insurance policies;

- Transactions involving high-risk countries, including those involving “own funds” transfers, particularly in circumstances in which there are no clear reasons for the specific transaction routing;
- Frequent or unexplained changes in ownership or management of Business Relationships;
- Illogical changes in business activities, especially where high-risk activities are involved;
- Situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide CDD documentation or provide documentation that is false, misleading, fraudulent or forged.

When reporting an STR in the GoAML system, the Company is required to select the most appropriate reason for reporting available from the menu selection provided. More than one reason may also be provided, if deemed necessary. In order to select the appropriate indicator, click ‘Add’ to select the appropriate reason for the report.

Select the reason(s) applicable and then press ‘Close’. Alternatively, the Company search for reasons using the search bar available on the top left when expanding the form. It is imperative that a minimum of one reason for reporting must be selected to avoid rejection of the report by the GoAML system.

26.3. INTERNAL SUSPICIOUS TRANSACTIONS REPORT - ISTR

Each employee is responsible for monitoring and reporting suspicious transaction to the Compliance department.

In case of identifying a transaction as unusual or suspicious at the time when the customer is at the company, our employee will proceed as follows:

- Conceal suspicions from the customer.
- Hold the transaction.
- Report to the transaction to the Compliance Officer in confidence.
- Share copy of the customer’s identification document and any document relating to the transaction to the Compliance Officer.
- Proceed as instructed by the Compliance Officer.
- Will not inform the customer that his transaction is being investigated or reported as a suspicious transaction. Such an action constitutes tipping-off and is a criminal offense.

By way of guidance, ISTRs should:

- Be timely, clear, concise, accurate and relevant.
- Cover the essential elements of who, what, when, where, why and how.
- Include a detailed description of the known or suspected criminal violation or suspicious activity in chronological order.

- Link the ISTR with any previously submitted ISTR if applicable.

26.4. SUSPICIOUS TRANSACTIONS IDENTIFIED BY THE COMPLIANCE DEPARTMENT

- Compliance officer is responsible for monitoring all high value transactions, high count transactions, PEP (Domestic/Foreign) transactions and high-risk jurisdiction transactions on a monthly basis.

- Compliance officer will monitor Customer activity for unusual size, volume, pattern or type of transactions, considering risk factors and red flags that are appropriate to our business. The Compliance Department will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.
- The Compliance Officer should conduct an appropriate investigation and review relevant information from internal or third-party sources before a STR is filed.

- In the case of an internally submitted iSTR, the compliance officer will conduct an in-depth investigation and may decide to either close or keep the case open for future monitoring, and if there are reasonable grounds for suspicion, the case will be submitted to the FIU.

Question to Ask Yourself

The following factors should be considered when seeking to identify a suspicious transaction. This list is not meant to be exhaustive.

- Does the transaction match with the customer's normal activity known to the company, the markets in which the customer is active and the customer's own business? (i.e. does it make sense?)

- Is the transaction in line with common practices in the market to which it relates to? (i.e. with reference to market's size and frequency?

- Is the role of the agent involved in the transaction unusual?

- Is the transaction to be settled in the normal manner?

- Are the reasons for the transactions comprehensible (i.e., might there be an easier, cheaper, or more convenient method available?)

26.5. TIMING OF SUSPICIOUS TRANSACTION REPORTS (STR)

(AML-CFT Law 9; AML-CFT Decision 17.1(a), 21.2)

The Company is obliged to report STRs to the FIU without delay. Since it is the responsibility of the designated AML/CFT compliance officer to "review, scrutinise and study records, receive data concerning suspicious transactions, and take decisions to either notify the FIU or maintain the transaction," it follows that the STRs should be immediately reported once the suspicious nature of the transaction becomes clear. This means that the internal reporting of suspicious transactions to the compliance officer should be done directly once the suspicion or reasonable grounds for suspicion are established, and immediately the compliance officer has confirmed that the transaction (whether pending, in progress, or past) is suspicious, it should be reported.

26.6. RED FLAGS/INDICATORS OF SUSPICIOUS TRANSACTIONS

The following list of red-flag indicators of potentially suspicious transactions is therefore by no means exhaustive.

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 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 organisation (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 authorised 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.
- Requests payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or installment 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 effected 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:

- 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 jewellery for cash in small incremental amounts.
- Involves the barter or exchange of PMS (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 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 authorised 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).

The 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 PMS. The negotiable instruments may be sequentially numbered or purchased at multiple locations, and may frequently lack payee information.
- Is divided in to smaller parts or installments 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.

27. CONFIDENTIALITY AND PROHIBITION AGAINST "TIPPING OFF"

(AML-CFT Law Article 25; AML-CFT Decision Articles 17.2, 21.2, 31.3, 39)

When reporting suspicious transactions to the FIU, the Company is obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, the Company, and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

The Company ensures that all relevant information relating to STRs is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. The Company need to ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used for case management and notifications, secure information flows and guidance/training to all staff members involved.

It should be noted that the confidentiality requirement does not pertain to communication within the Company or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/FT.

Non-compliance is a criminal offence and the employee involved will be terminated, immediately. Additionally, he/she is personally subject to fines, imprisonment, or both. Employee and senior management of the Company is strictly prohibited from informing customers, other persons or third parties, either directly or indirectly, that their transactions are being monitored, investigated, or reported to the FIU of Executive Office as suspicious transactions. Such actions are considered "Tipping-Off" and is a criminal offence.

The Company's compliance department ensures, through ongoing training and detailed procedures, that all employees of the company are aware of the consequences of tipping-off,

which include immediate dismissal in addition to fines, imprisonment, or both. The staff is being provided adequate AML/CFT training to avoid Tipping off.

Tipping Off is a federal crime for the Company's or their managers, employees or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction. Any person violating this prohibition is liable to a penalty of no less than AED100,000 and no more than AED500,000 and imprisonment for a term of not less than six months.

Part - V

GOVERNANCE

28. STRUCTURE OF COMPLIANCE PILLARS

Policies and Procedures

- Development of the internal polices procedures and controls
- Risk Focused Policies
- Controls to Ensure Compliance
- Monitoring and Reporting Systems

Compliance Officer

- Rolls and Responsibilities of Compliance Officer
- Responsibilities of Compliance Department
- Sufficient time, resources and authority

Training & Awareness

- Training Based on Current Procedure and Systems
- Annual Training Plan
- Continues Professional Development (CPD)
- Money Laundering and Counterfeit Awareness

Independent Audit

- Sufficient Scope and Testing
- Reporting to the BODs
- Timely Action to address any concerns or weaknesses

29. ROLES AND RESPONSIBILITIES OF COMPLIANCE OFFICER

The Company has been appointed the dedicated compliance officer responsible for overseeing the AML and Compliance function of the company. The Compliance Officer (CO) is responsible for implementation and oversight of organisation's compliance with AML/CFT rules and regulations, staff training, etc.

The Company ensures that the CO:

- Be an Independent staff in the organization;
- Report directly to the Director;
- Be provided with sufficient resources including time, systems, tools and support staff depending on the nature, size and complexity of its business;
- Be provided with unrestricted access to all information related to products or services, business partners, correspondent agents, customers and transactions;
- Be independent and does not have any conflict of interest in performing its role.

Responsibilities of the Compliance Officer (CO)

- ✓ The Compliance Officer is in charge of reviewing, scrutinizing and reporting STRs.
- ✓ The Compliance Officer should ensure the quality, strength and effectiveness of the Organization's AML/CFT program.
- ✓ Establishing and maintaining AML/CFT policies and procedures.
- ✓ Ensuring that the organization complies with the applicable AML/CFT laws.
- ✓ Ensuring day-to-day compliance with own internal AML/CFT policies and procedures.
- ✓ Responding promptly to any reasonable request for information if made by the Competent Authorities.
- ✓ Acting as the main point of contact in respect of handling internal suspicious transactions reports from the employees and analyze them before reporting to FIU. He / She shall also be the main contact point for coordinating with FIU and other concerned bodies regarding AML / CFT.
- ✓ Submit the threshold (AED 55,000/-) Exceeded transactions on timely manner in to the GoAML System.
- ✓ Submit Suspicious Transaction Reports to the FIU in a timely manner.
- ✓ The Compliance Officer is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organisations, for reporting suspicions to the FIU.
- ✓ Cooperate with and provide the FIU with all information it requires for fulfilling their obligations.

- ✓ The Compliance Officer is in charge of informing and reporting to senior management on the level of compliance and report on that to the relevant Supervisory Authority.
- ✓ Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML / CFT matters (whether internal or external) and developing AML Training calendar for ensuring all staffs are adequately trained.
- ✓ Conduct regular gap analysis on new notices/regulations/best practices issued by regulatory bodies vis-à-vis this AML Compliance policy.
- ✓ Ensure all key documents pertaining to KYC of customers, customer transactions and STR are retained for the minimum period of 5 years.
- ✓ The Compliance Officer is responsible to file the STR in GoAML System and coordinate with regulators for further investigation process.
- ✓ Working with senior management and other internal and external stakeholders to ensure that the Company's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

30. ROLES AND RESPONSIBILITIES OF THE OWNER

- ✓ Overall responsible for implementing the robust compliance program across each business product, counterparty, country in which it deals, delivery channel of its services, customers etc.
- ✓ Ensures that the company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- ✓ Approves the overall business risk assessment for the Company.
- ✓ Approves the AML/CFT policy.
- ✓ Reviews the compliance issues raised by the compliance department.
- ✓ Ensure day-to-day compliance with own internal AML/CFT policies and procedures are compiled and monitored by Compliance Officer.
- ✓ Ensure the Cooperation with and provide the FIU with all information it requires for fulfilling their obligations.
- ✓ Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters (whether internal or external) and developing AML Training calendar for ensuring all staffs are adequately trained.
- ✓ On-going monitoring of what may, in his opinion, constitute high-risk customer accounts, suspicious customers/transactions.
- ✓ Ensure that CO is maintaining all necessary CDD, transactions, STR and staff training records for the required periods.
- ✓ Ensure all key documents pertaining to KYC of customers, customer transactions and STR are retained for the minimum period of 5 years.

Part - VI

TRANSACTION MONITORING

31. TRANSACTION MONITORING

A well- defined transaction monitoring program is an important component of an effective AML & CFT program. The primary objective of the Company is to concentrate on actual risks, customer and product classification and to reduce the number of chances of company from being misused.

Basic Rules for Transaction Monitoring:

The 5 "W" s are:

a) *Who - is the customer- individual or corporate, what is the profile of the customer?*
b) *What - product is the customer availing, Gold, Diamond or any other product?*
c) *Where - is the customer remitting funds to? Is the country a high-risk jurisdiction? Is there a valid reason for remitting funds?*
d) *Why - is the customer remitting funds? Does the transaction make economic sense and what is the exact purpose?*
e) *Whom – for whom is the transaction being conducted, who will benefit from the transaction? Who is the Ultimate beneficiary?*

Our compliance department adopts a risk-based approach to transaction monitoring, which include the following components:

Scrutiny of customer transactions to ensure that the transactions are in line with the knowledge of the customer, his business, risk profile, source of wealth and funds.

Concern officer will review of customer records to ensure that documents, data and information collected during the KYC, CDD and monitoring processes are relevant and up to date.

The compliance department investigate any unusual or suspicious transactions and maintain all supporting records for a minimum period of 5 years.

Following the investigation of unusual transactions, if there are reasonable grounds for suspicion, our Compliance Officer will immediately report such transactions to FIU.

32. TRANSACTION MONITORING PROCEDURE

Data Collection: Gather transactional data, including transaction amounts, parties involved, timestamps, and any other relevant information necessary for analysis. This data can be sourced from internal systems, such as transaction databases or financial records.

Defining Risk Indicators: Define a set of risk indicators or red flags that will be used to identify potentially suspicious transactions. These indicators can be based on regulatory requirements, industry best practices, or specific risk factors relevant to the organization's business operations.

Analysis: Review transactions one by one, applying the defined risk indicators and examining transactional patterns, customer behavior, and other relevant factors. This analysis requires expertise and knowledge of AML/CTF regulations, emerging trends, and the organization's risk appetite.

Documentation: Document the findings, analysis, and any actions taken during the manual transaction monitoring process. Maintain detailed records that capture the rationale behind decisions made, the assessment of suspicious activities, and any follow-up actions required.

Investigation and Reporting: If suspicious transactions are identified, conduct further investigation to gather additional information and assess the level of risk or potential financial crime involved. If necessary, report the findings to the appropriate internal teams or authorities in compliance with regulatory requirements.

Escalation and Remediation: Establish clear protocols for escalating identified risks or suspicious activities to higher management or the designated AML compliance officer. Develop procedures for initiating remedial actions, such as customer due diligence updates, transaction blocking, or reporting to regulatory authorities.

Ongoing Monitoring and Review: Continuously monitor transactions, reassess risk indicators, and update the manual transaction monitoring process as needed. Regularly review the effectiveness of procedures, identify any areas for improvement, and incorporate lessons learned from investigations and regulatory developments.

By following these transaction monitoring procedures, organizations can enhance their ability to detect and mitigate potential risks related to money laundering, terrorist financing, and other financial crimes. It is important to note that organizations may also utilize automated transaction monitoring systems in conjunction with manual processes to improve efficiency and effectiveness in detecting suspicious activities.

33. CASH REPORTING MEASURES

A well- defined transaction monitoring program is an important component of an effective AML & CFT program. The primary objective of the Company is to concentrate on actual risks, customer and product classification and to reduce the number of chances of company from being misused.

To ensure compliance with cash reporting requirements, the following measures should be implemented for transactions equal to or exceeding AED 55,000:

Cash transactions with resident individuals:

Any cash transactions with resident individuals, whether it is in the form of purchases or sales, that equal or exceed AED 55,000 should be subject to scrutiny and due diligence measures, despite the company not primarily dealing with cash transactions.

Cash transactions with non-resident individuals:

Any cash transactions with non-resident individuals that equal or exceed AED 55,000 should be subject to heightened scrutiny and due diligence measures, despite the company not primarily dealing with cash transactions.

Cash transactions with legal entities:

Any cash transactions with legal entities, such as legal persons or businesses, that equal or exceed AED 55,000 should be subject to enhanced due diligence measures, despite the company not primarily dealing with cash transactions.

Part - VII

RECORD KEEPING

34. RECORD KEEPING

34.1. OBLIGATIONS AND TIMEFRAME FOR THE RETENTION AND AVAILABILITY OF RECORDS

AML-CFT Law (16.1 and AML-CFT Decision Articles 7.2, 24, 36, 37.3)

The Company is obliged to maintain detailed records, documents, data and statistics for all transactions, all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures. The Company is maintaining the records of all transactions and copies of supporting documents should be preserved and details such as Customer IDs, Trade Licenses, Invoice details, EDD Documents, Account Opening Documents, Customer Profiles etc. in an organized fashion so as to permit data analysis and the tracking of transactions, and to make the records available to the Competent Authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, depending on the circumstances, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account with the Company;
- Completion of a casual transaction (in respect of a customer with whom no Business Relationship is established);
- Completion of an inspection of the records by the Supervisory Authorities;
- The issue date of a final judgment by the competent judicial authorities;
- Liquidation, dissolution, or other form of termination of a legal person or arrangement.

34.2. TYPE OF RECORDS

Transaction Records

This category relates to operational records, documents and information concerning all transactions processed by the Company, whether domestic or international in nature.

CDD & EDD Records

This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:

- Customer Information, including account files and business correspondence, and results of any analysis undertaken
- Company Information
- Ongoing Monitoring of Business Relationships
- Suspicious Transaction Reports (STRs)

- Suspicious Activity Reports (SARs)
- DPMS Reports

35. ONGOING MONITORING OF BUSINESS RELATIONSHIPS

The compliance officer continually monitors the client profiles, transaction patterns as a part of ongoing monitoring process also keep updates the KYC details time to time in order to maintain the valid documents.

Additionally, the compliance department maintains below procedures:

- Records of transaction review, analysis, and investigation files, with their related correspondence;
- Customer correspondence call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to those transactions or their analysis and investigation;
- CDD records, documents, profiles or information gathered in the course of reviewing, analyzing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;
- Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.

36. ANTI-BRIBERY POLICY

The Company strictly prohibits any form of bribery and corruption within the company, as well as with its business partners, service providers, customers as well as governmental agencies.

The Company takes a zero-tolerance approach to bribery and corruption and very committed to acting professionally, fairly and with integrity in all our business dealings and relationships. It is our best practice objective that those we do business will take a similar zero-tolerance approach to bribery and corruption.

37. EXIT POLICY AND PROCEDURE

This policy and related procedures provide a clear exit process ensuring that clients are well informed, supported and smoothly transitioned from the Company.

Voluntary Client Exit

- Client no longer wishes to avail services provided by the Company.

Involuntary Client Exit

- When any suspicious activity is identified.
- When client enters sanctions list, is blacklisted, or involved in negative media news.
- When client is indulged in illegal activities
- If the client is reluctant to provide complete KYC or other supporting documents.
- If the client provided any manipulated, fake documents etc.
- If the Corporate Client has not executed transactions within 6-month interval from the date of account opening or date of last transaction with the Company.

Part - VIII

KNOW YOUR EMPLOYEE (KYE)

38. KNOW YOUR EMPLOYEE

As a part of Know Your Employee (KYE) process the organisation do screen the candidate's name against sanctions and PEP lists before we issue the offer letter. Following information should be obtained by the company before hiring any new employee: -

- Identity Check / Passport Check
- Criminal Check (Good Conduct Certificate from Police of UAE/countries where the employee will be joining, for the last 5 years)
- Credit Check & Civil Litigation Check: Al Etihad Credit Bureau in UAE and other similar agencies in countries, where the candidate is joining from (if applicable).
- Education Qualification Check: We only take the attested document of their educational qualification. In case the job does not require educational qualification, we waive this clause off.
- Reference Check: We perform a reference check on the employee's previous employers.

39. EMPLOYEE RESPONSIBILITIES

- Always be vigilant – report knowledge or suspicion of Money Laundering.
- Know Your Customer (KYC)
- Establish true owner of funds
- Proper completion and approval of forms.
- Question legitimacy when in doubt.
- Report potentially suspicious or unusual transactions and activities
- Data input.
- Follow all internal circulars and instructions.
- Adhere to our Anti-Money Laundering policy and procedures.
- Be accountable for your actions & Know your obligation – Ignorance is not an excuse.
- Not to knowingly assist in the laundering of criminal funds.
- Not to alert a suspected launderer.

40. STAFF TRAINING AND AWARENESS

In order to maintain an effective AML & CTF program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this

goal, the Compliance Officer or a third party provides annual AML training to all relevant employees.

We segregated the Training and Awareness based on the followings;

- Training for New Employees
- On-Going Training Sessions (For Exist Employees and Senior Management)
- Continues Professional Development (for Compliance Department)

- In order to maintain an effective AML & CTF program, it is imperative that all our employees understand this policy and are trained to identify and report suspicious activity. To achieve this goal, the CO or a third party provides annual AML training to all relevant employees.
- A comprehensive training must be provided to all employees including its manager in charge, functional heads and owners/partners/shareholder.
- The periodic training of all employees covers this policy, the KYC procedures, UAE and global regulations, particularly the identification and reporting of suspicious transactions.
- We provide AML training to all relevant employees within 30 days of joining the company. Relevant employees include employees with customer contact, operational staff as well as senior management.
- Refresher Training must be provided to all employees at regular intervals to remain updated with any changes in provisions, regulations and AML/CFT law.
- Objective and content of the AML Training program will be responsibility of the CO.
- Development of training program and calendar shall be the responsibility of Compliance Officer and submitted to the Compliance Committee for approval.
- The senior management ensures that the Compliance Officer and other employees of the compliance department must attend external training in AML/CFT compliance every year.

<u>The AML-CFT training will include, at a minimum:</u>

- Money laundering and terrorist financing, definitions, typologies as well as recent trends.
- AML/CFT policies and procedures including the highlights on recent changes.
- The regulatory responsibilities and obligations of employees under AML/CFT Laws, Regulations, Notices and the Standards.
- Description of Know Your Customer (KYC).
- Due Diligence measures and procedure for monitoring transactions.
- Sanction screening and PEP screening procedures.
- Red flags to identify unusual transactions or transaction patterns or customer behavior.

- Processes and procedures of making internal disclosures of unusual transactions.
- Roles of the Compliance Officer and Alternate Compliance Officer including their full contact details.
- Tipping off.
- Record retention policy.
- Reference to industry guidance and other sources of information.
- Penalties for non-compliance with the AML/CFT Laws, Regulations, Notices and the Standards.
- Disciplinary procedures to be applied on employees for not adhering to the AML Policy and Procedures.
- And, any Updating and Regulations from the Regulator and the relevant Government Authorities.

41. INDEPENDENT INTERNAL AUDIT

(AML-CFT Decision Article 20.6)

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. The Company is obliged to have in place an independent audit function to test the effectiveness and adequacy of the internal polices, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organisations. In this regard, the Company ensures that the independent audit function is appropriately staffed and organized, and that it has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/FT risks to which the company is exposed, and with the nature and size of the businesses.

The Company ensures that the periodic inspection and testing of all aspects of the AML/CFT compliance programmes, including ML/FT business risk assessment and AML/CFT mitigation measures, and CDD policies, procedures and controls, is incorporated into the regular audit plans.

The Compliance functions are regularly audited by Internal Audit and the report submitted to the director. The Compliance Officer and other responsible personnel involved to ensure all the open audit points are satisfactorily closed and updates on a timely basis.

The independent audit functions include the following:

- Internal Audit Charter, Scope and Methodology of Audit
- Adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.

- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity
- Submit the report directly to the Director.

Part - IX

VIOLATIONS AND ADMINISTRATIVE FINES

42. VIOLATIONS AND ADMINISTRATIVE FINES

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 that are Subject to the Supervision of the Ministry of Justice and the Ministry of Economy.

No.	Article	Violation	Administrative Fine
1	Article (4) Clause 1	Failure to undertake the actions and procedures necessary to identify the risks associated with the crime in the violator's field of work.	100,000 AED
2	Article (23)	Failure to identify and assess the risks that may arise in the violator's field of work when developing the services that the violator offers or when conducting new professional practices through its facility.	100,000 AED
3	Article (4) Clause 2	Failure to undertake the actions and procedures necessary to mitigate the risks identified based on the results of the National Risk Assessment or the Self-assessment process given the nature and scale of the violator's business.	50,000 AED
4	Article (20)	Failure to implement internal policies, procedures and controls within the facility aimed at combating crime or preventing involvement in suspicious business relationships.	50,000 AED
5	Article (4) Clause 2/B + Article (22) Clause 1	Failure to take the necessary enhanced due diligence measures to manage high risks.	200,000 AED
6	Article (4) Clause 3	Failure to take the necessary simplified due diligence measures to manage low risks.	50,000 AED
7	Article (5)	Failure to undertake the necessary customer due diligence measures before establishing the business relationship or resuming a business relationship or performing a transaction under the customer's name or in his/her favor.	100,000 AED
8	Article (8) Clause 3	Failure to undertake the necessary measures to understand the purpose of the business relationship and its nature, or the failure to acquire any information pertaining to this purpose when needed.	50,000 AED
9	Article (8) Clause 4	Failure to undertake the necessary measures to understand the nature of the customer's business, the ownership structure of his/her business, and the extent to which the customer has control over that business.	50,000 AED

10	Article (8) Clause 1 and 2	Failure to verify the identity of the customer and the real beneficiary or their representative using documents or data collected from reliable and independent sources before or while establishing a business relationship or opening an account or prior to performing a transaction for a customer with whom no business relationship has been established.	100,000 AED
11	Article (7)	Failure to undertake the due diligence measures pertaining to the ongoing supervision of customers while conducting the business relationship.	50,000 AED
12	Article (13)	Failure to notify the Financial Intelligence Unit of the suspicious transaction report when the customer due diligence measures were not taken before establishing or continuing a business relationship with the customer or performing a transaction for the customer or under his/her name.	200,000 AED
13	Article (17) Clause 1/A	Delay in notifying the Financial Intelligence Unit of the suspicious transaction report in case there is suspicion or if there are reasonable grounds to suspect that the business relationship with the customer is in whole or in part linked to the crime, or that the customer's funds that are subject to the business relationship are in fact proceeds of a crime or were used in committing a crime.	100,000 AED
14	Article (17) Clause 1/A	Failure to provide the Financial Intelligence Unit with the additional information it requires regarding the matter reported in the suspicious transaction report.	200,000 AED
15	Article (14) Clause 1	Dealing with shell banks in any way.	1,000,000 AED
16	Article (14) Clause 2	Opening or maintaining bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.	1,000,000 AED
17	Article (15)	Failure to conduct due diligence measures on politically exposed persons before establishing or continuing a business relationship with such customers.	100,000 AED
18	Article (18) Clause 1	Disclosing, directly or indirectly, to the customer or any other person(s) that they have reported or are intending to report a suspicious transaction.	200,000 AED
19	Article (21)	Failure to appoint a compliance officer	50,000 AED
20	Article (19)	Failure to implement the measures prescribed by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal	200,000 AED

		Organizations with respect to customers from high-risk countries.	
21	Article (24) Clause 1	Failure to create records for keeping track of financial transactions with customers.	100,000 AED
22	Article (24) Clause 3	Failure to create records that keep track of financial transactions with the customers in an organized manner, which prevents data analysis and tracking of financial transactions	50,000 AED
23	Article (24) Clause 2	Failure to keep records and documents related to the financial transactions for a period of five years from the date of concluding the transaction or terminating the business relationship with the customer, or from the date of completion of the inspection of the customer's facilities.	50,000 AED
24	Article (24) Clause 4	Failure to make all the information pertaining to the customer due diligence, ongoing supervision, and the results of their analysis, records, files, documents, correspondence and forms available to the competent authorities upon request.	50,000 AED
25	Article (21) Clause 4	Failure to provide training for the facility's employees on combating money laundering and the financing of terrorism.	50,000 AED
26	Article (60)	Failure to take the necessary measures regarding customers included in the international or domestic sanctions lists before establishing or continuing a business relationship with those customers.	1,000,000 AED

Part - X

APPENDICES

43. GLOSSARY OF TERMS

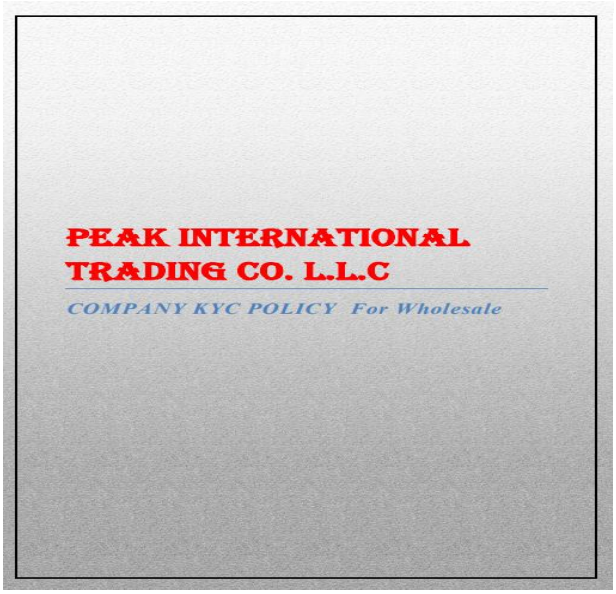
Term	Definition
Beneficial Owner	Natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal 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.
Crime	Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organisations
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 Organisations
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 Organisations.
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 favour of another form of Legal Arrangement. (e) Working or equipping another person to act as a nominal shareholder in favour of another person. 5. Other professions and activities which shall be determined by a decision of the Minister
FATF	The Financial Action Task Force is an intergovernmental 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.
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.
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 Organisations	Organisations whose establishment is criminalised or which exercise a criminalised activity.
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 organisation or any prominent function within such an organisation; 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 misdemeanour 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.
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
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.
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 organisations, whether committed or attempted.

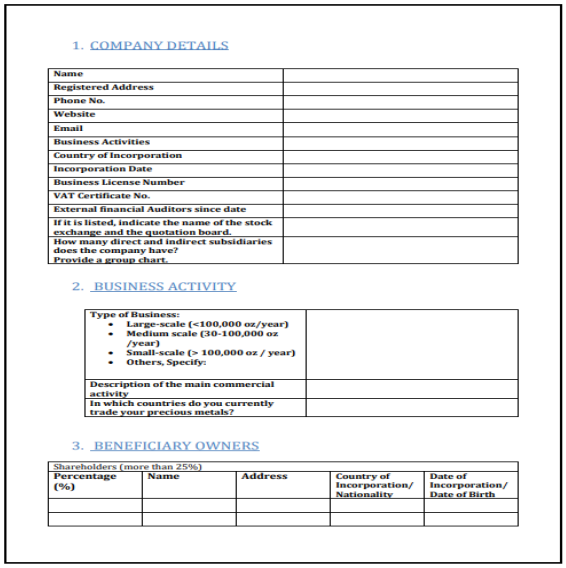
TFS	Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

44. FORMS



PEAK INTERNATIONAL TRADING CO. L.L.C

COMPANY KYC POLICY For Wholesale



1. COMPANY DETAILS

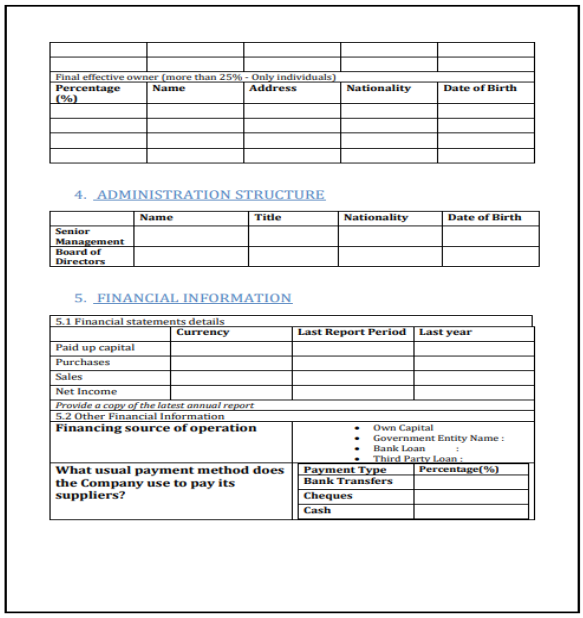
Name	
Registered Address	
Phone No.	
Website	
Email	
Business Activities	
Country of Incorporation	
Incorporation Date	
Business License Number	
VAT Certificate No.	
External financial Auditors since date	
If it is listed, indicate the name of the stock exchange and the quotation board.	
How many direct and indirect subsidiaries does the company have? Provide a group chart.	

2. BUSINESS ACTIVITY

Type of Business: • **Large-scale (<100,000 oz/year)** • **Medium scale (30-100,000 oz /year)** • **Small-scale (> 100,000 oz / year)** • **Others, Specify:**	
Description of the main commercial activity	
In which countries do you currently trade your precious metals?	

3. BENEFICIARY OWNERS

Shareholders (more than 25%)				
Percentage (%)	**Name**	**Address**	**Country of Incorporation/ Nationality**	**Date of Incorporation/ Date of Birth**



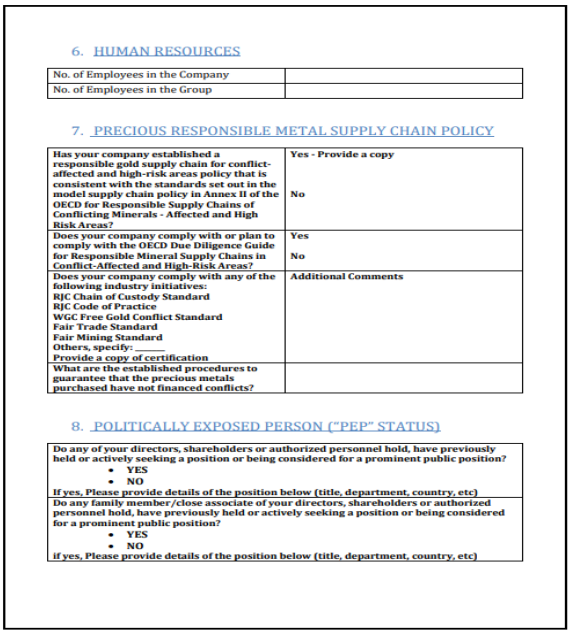
Final effective owner (more than 25% - Only individuals)				
Percentage (%)	**Name**	**Address**	**Nationality**	**Date of Birth**

4. ADMINISTRATION STRUCTURE

	Name	**Title**	**Nationality**	**Date of Birth**
Senior Management				
Board of Directors				

5. FINANCIAL INFORMATION

5.1 Financial statements details			
	Currency	**Last Report Period**	**Last year**
Paid up capital			
Purchases			
Sales			
Net Income			
Provide a copy of the latest annual report			
5.2 Other Financial Information			
Financing source of operation	• Own Capital • Government Entity Name : • Bank Loan : • Third Party Loan :		
What usual payment method does the Company use to pay its suppliers?	**Payment Type**	**Percentage(%)**	
	Bank Transfers		
	Cheques		
	Cash		



6. HUMAN RESOURCES

No. of Employees in the Company	
No. of Employees in the Group	

7. PRECIOUS RESPONSIBLE METAL SUPPLY CHAIN POLICY

Has your company established a responsible gold supply chain for conflict-affected and high-risk areas policy that is consistent with the standards set out in the model supply chain policy in Annex II of the OECD for Responsible Supply Chains of Conflicting Minerals - Affected and High Risk Areas?	**Yes - Provide a copy** **No**
Does your company comply with or plan to comply with the OECD Due Diligence Guide for Responsible Mineral Supply Chains in Conflict-Affected and High-Risk Areas?	**Yes** **No**
Does your company comply with any of the following industry initiatives: **RJC Chain of Custody Standard** **RJC Code of Practice** **WGC Free Gold Conflict Standard** **Fair Trade Standard** **Fair Mining Standard** **Others, specify: ___** **Provide a copy of certification**	**Additional Comments**
What are the established procedures to guarantee that the precious metals purchased have not financed conflicts?	

8. POLITICALLY EXPOSED PERSON ("PEP" STATUS)

Do any of your directors, shareholders or authorized personnel hold, have previously held or actively seeking a position or being considered for a prominent public position? • **YES** • **NO**
If yes, Please provide details of the position below (title, department, country, etc)
Do any family member/close associate of your directors, shareholders or authorized personnel hold, have previously held or actively seeking a position or being considered for a prominent public position? • **YES** • **NO**
if yes, Please provide details of the position below (title, department, country, etc)

Definition of "PEP"

Entrusted with prominent public functions, for example Heads of State or of government, a government minister, a senior public servant, a senior judicial or military official, a senior executive of a state-owned corporation, a member of the legislature, a senior official of a political party, or a member of the senior management of an international organization.

9. ADDITIONAL DISCLOSURE

Have any of the directors, shareholders, or authorized personal been the subject of any proceedings of a disciplinary or criminal nature or have been notified of any potential proceedings or investigation, under any law in any jurisdiction? • YES • NO **If yes, Please describe below :**
Have any directors, shareholders or authorized personal been convicted for any offence or is being subject to any pending proceedings relating to money laundering or terrorist financing? • YES • NO **If yes, Please describe below :**
*** If the answer to the above is "Yes", please provide supporting documents. Where appropriate, to provide all relevant particulars.**

10. AML/CFT

Is your company subject to the Money Laundering / Anti-Financial Terrorism Law / Regulation?	**Yes - Provide a copy** **No**
Name of the AML-CTF Law / Regulation	
Regulator's Name	
Has your company established a compliance program that contains AML/CFT policies and procedures, in accordance with internal and international laws, regulations and standards?	**Yes - Provide a copy** **No**

11. BRIBERY POLICY

Does your company have a bribery policy?	**Yes - Provide a copy**
	No
Has the company or Senior Management anywhere in the world ever been charged with violating applicable anti-bribery laws or regulations?	**Yes - Provide a copy** **No**

12. DECLARATION

I/We hereby declare that the information provided above is true, correct and complete as on date of writing to best of my knowledge and that all documents submitted along with this application are genuine.

Further, I/We hereby undertake to automatically and immediately inform **PEAK INTERNATIONAL TRADING CO. L.L.C** of any material changes in the information provided herein and agree that **PEAK INTERNATIONAL TRADING CO. L.L.C** is neither responsible nor liable for any losses or activity performed on the basis of the information provided.

I/We also agree to provide any additional information or documentation that may be required from time to time by **PEAK INTERNATIONAL TRADING CO. L.L.C** or its authorized agents or representatives.

	Authorized Signatory
Signature	
Print Name	
Title	
Company's Stamp	
Date and Location	

DUE DILIGENCE REQUIREMENTS

- Certificate of Incorporation
- Memorandum and Articles of Association
- Trade License
- Full details of Beneficial owners if not mentioned in MOA & AOA.
- ID and Proof of Address of any Beneficial Owners - own 25% or more of the Company and not a Director (see below).
- List of directors if not mentioned in MOA & AOA.
- List of Authorized Signatures (on letterhead and signed by your authorized signatories)
- List of Authorized Traders
- Registered Address of the Company
- Anti-Money Laundering Policy/ Anti Bribery and Corruption policy.
- Standing Settlement Instruction (SSI)/ Bank account details on your letterhead.

- Latest Audited Financials – If the Company is newly established and no Audited Financials are available then a copy of a recent Bank account statement will be required.
- VAT Certificate.

Documents do not need to be certified, however wherever possible an employee or representative of **PEAK INTERNATIONAL TRADING CO. L.L.C** should verify the IDs of the Directors.

ON LETTER HEAD

To

Date: .....

PEAK INTERNATIONAL TRADING CO. LLC
Dubai - UAE.

Dear Sirs,

Subject: AUTHORIZATION LETTER

We hereby authorize the following personnel as our representative to deal with **Peak International Trading Co. LLC** on our behalf. They have authority to carry-out the following:

☑ **Delivery/ Collection of gold**
☑ **Signing/ issuing receipts/payments, vouchers, signing statements in connection with the precious metals transactions and the payment/ receipt thereto**
☑ **Collecting cheques/ other documents in connection with delivery of gold**
☑ **Trading - Fixing gold rates, placing/ amending/ cancelling orders.**

S #	Name	ID No. & Mobile No.	Specimen Signature
1.			
2.			

Note: The valid Passport/ Emirates ID (if UAE entity) copy of the above is attached.

This authorization is valid with effect from today and until revoked in writing.

Thanking you,

For .....

ON LETTER HEAD

Date:

OPENING OF ACCOUNT

A meeting was held between the Board of Directors of ..... on date ..... at our office.

During the meeting it was resolved to OPEN and OPERATE an account with **PEAK INTERNATIONAL TRADING CO. (L.L.C)** in the name ..... of herein after called as the company.

It was also resolved to avail all buying and selling facilities of gold in the form of Bars, Coins, etc.

It was resolved that ..... , having passport number ....., is/are authorized to carry out all necessary operations including sign all account related documents singly and all other related operations with respect to the company's account with **PEAK INTERNATIONAL TRADING CO. LLC.**

In addition he is authorized to sign in the representative letter on behalf of our company. In case of any kind of gold dealings and financial transactions should be engaged by receiving a separate letter of List Authorized Person/s signed by the company owners/partners.

Signed an on behalf of:

Authorized Signatory

Name :

Company Name:

Stamp:

ON LETTER HEAD

POLITICALLY EXPOSED PERSON (PEP)DECLARATION FORM

The information in this form is collected in order to comply with the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities requirement.

A politically exposed person (PEP) is an individual who is or who has been entrusted with prominent public functions domestically' or by a foreign county.

Prominent public functions include the following profiles:

1. Head of State or of Government
2. Senior politician
3. Senior government, judicial or military official
4. Member of ruling royal family
5. Senior executive of state-owned corporation / government linked company
6. Important political party official

The definition of PEP also includes immediate family members, relatives, adviser, personal adviser or business associate of an individual stated above

1. Are you a PEP? Yes☐ No☐
2. Is you or the entity related to a PEP? Yes☐ No☐

(Please fill the below questions if the first two questions you answered - yes)

3. If you are or related to a PEP, please indicate the profile and relationship to you:

A. Head of State or of Government ☐
B. Senior politician☐
C. Senior government, judicial or military official ☐
D. Member of ruling royal family☐
E. Senior executive of state-owned corporation / Government linked company☐
F. Important political party official☐
G.Other……

I hereby declare that the details and information given to Peak International Trading Co. LLC are complete and true to the best of my knowledge.

Name:

Designation:

Company Name:

Date:

Signature:

Date

To,

……

Subject: Undertaking letter regarding Source of Funds

Dear Sir/Madam,

I am writing this letter to confirm the source of funds that will be used for gold jewellery trading.

The funds that I will be using have been acquired through income from my business. I declare that the funds are legitimate and do nothave any illegal origin.

I understand that your entity has an obligation to comply with the laws and regulations on money laundering and terrorist financing. I assure you that the funds used to purchase your products are from legitimate sources.

If necessary, I am willing to provide any additional documentation or information to support the legitimacy of the funds.

Please let me know if you need any further clarification or information.

Thank you for your understanding and cooperation.Sincerely,

_____

For
Company:
Name:
Designation:

UNDERTAKING LETTER

Date:

To,

PEAK INTERNATIONAL TRADING CO. LLC OFFICE 309, GOLD LAND BUILDING DUBAI, U.A.E.

WHOMSOEVER IT MAY CONCERN

Dubai, UAE

Dear Sir,

I, …… , ….. , National having Passport number ….. , Owner/ UBO of ……

I hereby confirm that neither of our entities nor any of our related parties are dealing with sanctioned countries listed by UAE, United Nations, United States, European Union or the UK, nor Owned or controlled by, or operating as agents of the Governments of Cuba, Iran, North Korea, Syria or Venezuela or Resident or domiciled in Iran, Syria, North Korea, Cuba or Crimea.

I hereby further confirm that all of our business operations have never dealt with / won't involve a sanctioned countries as & when notified by UAE, United National, United States, European Union or the UK or violate or to cause any economic or financial sanctions or trade embargoes implemented, administered or enforced by the United Arab Emirates, The United Nations, United States, European Union, United Kingdom or other relevant sanctions authorities.

I also confirm that neither I nor any of key person acting as nominee of any person national/ residing any of the above sanctioned countries.

Finally, I confirm that the funds used to sale/purchase Precious Metals & Stones to/from doesn't consist of money which is derived from the proceeds of Criminal activities / from means of any illegal source.

Thanking you.

Yours' faithfully,

For & on Behalf of ……

NAME AND SIGN OF AUTHORISED PERSON:

WITH COMPANY STAMP: