ASHKENAZI TRADING DMCC

AML/CFT POLICIES & PROCEDURES

March 2025

CONFIDENTIALITY STATEMENT

Table of Contents

POLICY STATEMENT

Ashkenazi Trading DMCC (hereinafter referred as the "**Company**" or "**Ashkenazi Trading**") is a licensed entity and supervised by the Ministry of Economy, UAE as its reporting entity and is committed to preventing money laundering and countering the financing of terrorism.

Ashkenazi Trading as a business entity was established in 2023 and is registered with DMCC bearing license number DMCC-892596. The licensed activities as per Trade License are Non-Manufactured Precious Metal Trading Company.

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

The management of **Ashkenazi Trading** believes that the best way to fulfill this commitment is to establish effective internal policies and procedures that are conducive to:

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

List of other policies to be considered as part of the AML Policy:

- **Supply Chain Policy**
- **Anti-Bribery and Anti-Corruption Policy**
- **AML Governance Framework**
- **Cash Acceptance Procedure**
- **Red Flag Indicators**
- **Suspicion Transaction Reports Procedures**
- **Targeted Financial Sanctions Policy**
- **Risk Identification and Assessment**

VERSION CONTROL

Version Name	Date of Version	Details of Amendment
V. 1.0	2023	First Policy was created
V. 2.0	2025	Policy updated as per the amendments and changes as enacted and mandated by Ministry of Economy, United Arab Emirates.

Document Title:	**AML/CFT POLICIES AND PROCEDURES**
Version	**Drafted and Approved by:**
V. 2.0	Money Laundering Reporting Officer (Assisted by the Specialized External Consultant)

1. INTRODUCTION

1.1. Ashkenazi Trading is a Designated Non-financial Business and Profession (DNFBPs) according to Article (3) of Cabinet Decision No. (10) Of 2019 concerning the Implementing Regulation of Decree Law No. (20) Of 2018 On 'Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations' and is therefore a reporting entity obligated to comply with applicable laws and regulations regarding Anti-Money Laundering (AML) and countering the financing of terrorism and financing of illegal organisations (CFT).

1.2. The senior management of our Company has adopted and approved this Policy Manual for Anti-Money Laundering and Countering the Financing of Terrorism and Financing of Illegal Organisations (this "Policy Manual" or "Compliance Policy" or "Manual") to comply with applicable laws and regulations in this regard.

1.3. The compliance policy serves as a guiding framework, reflecting our Company's commitment to prevent, detect, and mitigate the risks associated with money laundering and other financial crimes. It establishes the principles, procedures, and responsibilities that we adhere to in order to uphold legal and ethical standards, safeguard our reputation, and maintain the trust of our stakeholders.

1.4. The primary objective of this policy is to establish a robust and effective AML program that aligns with international standards, regulatory requirements, and best practices. It encompasses a wide range of measures designed to identify and assess money laundering risks, implement appropriate controls and procedures, monitor, and report suspicious activities, and provide ongoing training and awareness for our employees.

1.5. Through the implementation of this compliance policy, we aim to foster a culture of compliance within our Company. We believe that every employee plays a crucial role in preventing money laundering, and we provide them with the necessary knowledge and tools to fulfil their responsibilities effectively. Recognizing that combating money laundering requires a collective effort, we actively collaborate with relevant authorities, regulatory bodies, and industry partners to exchange information and enhance our effectiveness in combating financial crime.

1.6. As part of our commitment to continuous improvement, this policy will be regularly reviewed and updated to reflect changes in regulatory requirements, emerging risks, and evolving industry practices. We encourage all employees to familiarize themselves with the policy, seek clarifications when needed, and promptly report any concerns or suspicious activities through established reporting channels.

1.7. By implementing and adhering to this compliance policy, Our Company aims to contribute to global efforts in combating money laundering, the financing of terrorism, and the financing of illegal Organisations, thereby safeguarding the integrity of the financial system. We strongly believe that by taking these measures, our Company can foster a more transparent and secure business environment, while minimizing the risk of financial crimes.

1.8. By upholding the highest standards of compliance, ethics, and accountability, we strive to build a secure and trustworthy DPMS (Dealers in Precious Metals) industry in the UAE, attracting legitimate investment and promoting sustainable growth for the benefit of all stakeholders.

2. PURPOSE & RATIONALE

2.1. The purpose of this Policy is to outline the provisions, procedures, and controls mandated by national legislation regarding AML, CFT, and Financing of Illegal Organisations. All personnel are informed about the Policy's existence and its contents. They hold personal and corporate responsibility to report any AML/CFT concerns to the Compliance Officer.

2.2. The primary objective of this compliance policy is to implement measures and procedures that effectively prevent money laundering activities. Money laundering involves concealing the origins of illicit funds to make them appear legitimate, allowing criminals to enjoy the proceeds of their illegal activities. This compliance policy aims to detect and deter such activities. In addition to preventing money laundering, this policy serves the following purposes:

- **Compliance with National Legislation:** The policy ensures that our Company fully complies with the relevant national legislation pertaining to AML, CFT, and financing of illegal Organisations. It establishes the necessary controls and procedures to meet legal obligations and mitigate associated risks.
- **Risk Mitigation:** By implementing appropriate measures, such as customer due diligence, transaction monitoring, and suspicious activity reporting, the policy helps mitigate the risks associated with money laundering and terrorist financing. It ensures that our Company remains vigilant in identifying and addressing potential risks.
- **Enhance Risk Management:** Implementing a compliance policy enhances our Company's overall risk management framework by identifying and addressing money laundering and terrorist financing risks. The policy enables our Company to proactively manage potential threats, protect assets, and ensure compliance with regulatory obligations.
- **Protecting Reputation and Trust:** By maintaining a robust AML/CFT compliance program, our Company safeguards its reputation and maintains the trust of its stakeholders. The policy demonstrates Ashkenazi Trading's commitment to ethical business practices and a secure financial environment.
- **Supporting Global Efforts:** The policy aligns with global initiatives and efforts to combat money laundering and terrorist financing. By adhering to international standards, our Company contributes to the collective fight against financial crimes and supports a secure global financial system.
- **Combating the Financing of Terrorism:** Another important purpose of this compliance policy is to combat CFT. Terrorist Organisations rely on fundings to carry out their activities, and this compliance policy helps in identifying and preventing the flow of funds that can be used to support terrorist activities.

- **Protect Financial System Stability:** Money laundering and terrorist financing activities can destabilize the financial system by injecting illicit funds into legitimate channels. This compliance policy aims to protect the integrity and stability of the financial system by detecting and deterring such activities, thereby safeguarding the interests of our Company and the wider economy.
- **Training and Awareness:** The policy establishes the importance of ongoing training and awareness programs to ensure that all employees understand their responsibilities and are equipped with the knowledge to identify and report suspicious activities. It fosters a culture of compliance and ensures that our Company remains vigilant in preventing money laundering.

2.3. The Compliance Policy of our Company is driven by two key criteria to ensure the acceptance of business relationships:

- **Legitimate Source of Funds:** Our Company will only engage in business relationships where the sources of funds can be reasonably verified as legitimate. This necessitates conducting thorough due diligence and verification procedures to ensure that the funds being invested or transacted originate from legal and legitimate sources. By implementing these measures, Our Company aims to prevent money laundering activities and avoid unwittingly facilitating illicit financial transactions.
- **Risk to Reputation and AML/CFT Commitment:** Our Company will also assess the potential risks, both actual and potential, that a business relationship may pose to its reputation and its commitment to AML/CFT principles. This entails evaluating the background, reputation, and conduct of potential clients or partners to ascertain if they have any involvement or associations with activities that could potentially harm our Company reputation or compromise its commitment to AML/CFT standards.

3. SCOPE

3.1. The provisions, procedures, and controls outlined below are mandatory and apply to all employees, regardless of their function or location of work, as well as to all clients, including buyers, sellers, affiliates, and partners of our Company.

3.2. It is the responsibility of employees to adhere to the standards set by local and international regulatory agencies and to safeguard the Company's reputation by preventing any involvement in illegal activities. Violations of this Policy by employees or affiliates will be considered disciplinary offenses, and our Company reserves the right to take appropriate action, including additional measures, as deemed necessary to ensure the diligent implementation and enforcement of this Policy.

3.3. If our Company, its personnel, or its premises are inadvertently used for money laundering or other illegal activities, the Company may be subject to significant civil and criminal penalties. Therefore, it is crucial for every member, officer, director, and employee to be familiar with and comply with the processes and procedures outlined in this Policy.

3.4. If a client of our Company breaches any provisions of this Policy, our Company may take appropriate measures based on the severity of the violation. These measures may include issuing a warning,

suspending the operations of the client's account, terminating the client's account, or reporting the violation to the relevant authorities. The action taken will be determined in accordance with the seriousness of the breach and in compliance with applicable laws and regulations.

3.5. By implementing these measures, our Company aims to maintain a high level of compliance with AML/CFT and ensure integrity and reputation while fulfilling its obligations to prevent and detect any illicit activities.

4. DEFINITION OF MONEY LAUNDERING, FINANCING OF TERRORISM, AND ILLEGAL ORGANISATION

4.1. In recent years, the global community has increasingly recognized the significance of combating money laundering and terrorist financing. This concern has been fueled by factors such as globalization and advancements in technology. Organisations operating on a global scale are particularly susceptible to these risks due to their diverse offerings, extensive market reach, and interconnected distribution channels. The integration of the global financial and trade systems, along with the evolution of payment methods and relaxed restrictions on capital movement, has provided criminals with new avenues to engage in illicit activities.

4.2. The United Arab Emirates (UAE) has demonstrated a strong commitment to addressing these challenges. The UAE has taken significant steps to combat money laundering and terrorist financing by implementing robust regulatory frameworks, enacting legislation, and establishing regulatory authorities dedicated to AML and CFT. The country has also actively engaged in international collaborations and partnerships to enhance its capabilities in this area.

4.3. Through its proactive measures, the UAE aims to protect the integrity and stability of its financial system, prevent the misuse of financial resources for illicit purposes, and contribute to global efforts in combating money laundering and terrorist financing. The UAE recognizes the importance of a comprehensive and coordinated approach involving government agencies, financial institutions, and other stakeholders to effectively address these risks. By promoting transparency, conducting thorough due diligence, and adopting international best practices, the UAE seeks to create an environment that deters illicit activities and ensures the security and integrity of its financial sector.

Money Laundering

4.4. Money laundering refers to the act of engaging in financial or banking activities with the intention of disguising or altering the origin of unlawfully acquired funds. This is done by routing the funds through the financial and banking system in a way that makes them appear to come from legitimate sources, subsequently reinvesting and utilizing them in a lawful manner that contradicts their actual illicit nature.

4.5. In simpler terms, money laundering is the process of transforming illicitly obtained money into a legitimate and "clean" form. Criminals resort to money laundering to evade detection by law enforcement authorities and to exploit the illicit proceeds for personal use, including engaging in further criminal activities and investing in lawful enterprises.

4.6. 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") defines money laundering as engaging in any of the following acts willfully, or/and having knowledge that the funds are the proceeds of a felony or a misdemeanor (i.e., a predicate offence):

- Transferring or moving proceeds or conducting any transaction with the aim of 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.

Stages of Money Laundering

4.7. Although money laundering involves intricate and interconnected transactions that are challenging to unravel, it can generally be simplified into three main stages:

- **Placement:** This initial stage involves introducing illicit funds into the legitimate financial system. Criminals typically attempt to deposit or move the unlawfully obtained money in a way that conceals its origin. This may involve activities such as making cash deposits, purchasing assets, or using money transfer methods to place the funds into the financial system.
- **Layering:** In this stage, the aim is to obscure the paper trail and make it difficult to trace the illicit funds back to their illegal source. Multiple complex transactions, involving transfers between accounts, investments, or purchases, are employed to create layers of transactions that make it challenging for authorities to track the origin of the money.
- **Integration:** The final stage of money laundering involves merging the illicit funds back into the legitimate economy, giving them the appearance of being lawful. The laundered money is reintroduced into the financial system or invested in legitimate businesses or assets, making it difficult to distinguish between the illicitly obtained funds and legitimately earned income.

4.8. These three stages—placement, layering, and integration—constitute the general framework of money laundering, albeit with variations and complexities in individual cases.

Financing of Terrorism

4.9. The financing of terrorism follows a three-step process that includes collecting, transmitting, and distributing funds for terrorist activities. Initially, funds are raised through various means, both illegal and legal. These funds are then subjected to money laundering techniques, which involve passing them through the financial system to obscure their origin and intended destination.

4.10. Finally, the laundered funds are disseminated to terror cells, who utilize the money to acquire weapons, cover operational expenses, and further the objectives of the group. To evade detection and overcome preventive measures implemented by jurisdictions, terrorists constantly adapt their methods and locations for fundraising and moving funds and assets. Their goal is to evade safeguards

and detection mechanisms designed to identify and disrupt such activities. The AML/CFT Law defines Financing of Terrorism as:

- Engaging in any form of money laundering while being aware that the proceeds, either wholly or partially, belong to a terrorist Organisation or individual involved in terrorism, or are intended to finance such entities or terrorism-related activities. This applies even if there is no intention to conceal or disguise the illicit origin of the funds.
- Providing, gathering, preparing, or acquiring proceeds, or facilitating their acquisition by others, with the intention to use them or with the knowledge that such funds will be utilized, either wholly or partially, for the commission of a terrorist offense. This also encompasses carrying out these acts on behalf of a terrorist Organisation or individual involved in terrorism, while being aware of the true background or purpose behind these actions.

Financing of Illegal Organisations

4.11. The AML/CFT Law defines Financing of Illegal Organisations as:

- Engaging in any form of money laundering, while being aware that the proceeds, whether wholly or partially, are owned by an illegal Organisation or any individual associated with an illegal Organisation or are intended to finance such illegal activities or individuals. This applies even if there is no intention to conceal or disguise the illicit origin of the funds.
- Providing, gathering, preparing, obtaining proceeds, or assisting others in obtaining them, with the intention to use such proceeds or with knowledge that they will be used, either wholly or partially, for the benefit of an illegal Organisation or any of its members, while being aware of the identity or purpose of the Organisation.

5. LEGAL AND REGULATORY FRAMEWORK

National Legislative and Regulatory Framework

5.1. The United Arab Emirates (UAE) is strongly dedicated to combating the illicit activities of money laundering and terrorism financing. It is committed to detecting, deterring, and acting against these activities in accordance with the established legislation. The UAE has established competent authorities responsible for implementing an institutional framework to oversee, regulate, and gather information on all activities that could potentially contribute to financial crimes, including money laundering and terrorism financing.

5.2. With a strong commitment to preserving the integrity of the UAE's financial environment and combating illegal financing and corruption, the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations (NAMLCFTC) was established in 2000. Its primary role is to oversee and coordinate AML policies and initiatives in the UAE. The committee's focus is on enhancing the effectiveness of the AML and CFT framework within the country. It achieves this by ensuring ongoing compliance with international standards concerning the prevention and detection of money laundering and the financing of terrorist activities.

5.3. In August 2020, the Central Bank of the UAE (CBUAE) established a specialized department called the Anti-Money Laundering and Combating the Financing of Terrorism Supervision Department (AMLD). This department is responsible for handling all matters related to AML/CFT within the UAE. The AMLD works closely with the UAE's National AML/CFT Committee to effectively implement the National Action Plan.

5.4. As an active participant, the UAE plays a significant role in global efforts to combat money laundering and the financing of terrorism (AML/CFT). The country is dedicated to fully complying with the standards established by the International Financial Action Task Force (FATF). In 2018, the UAE conducted its first national risk assessment on money laundering and terrorist financing, which involved the participation of relevant authorities. The assessment identified areas with high risks in these domains.

5.5. To address the threats posed by AML/CFT, the UAE has enacted laws and implementation regulations. These legal frameworks aim to combat and mitigate the risks associated with money laundering and terrorist financing.

Federal Law

5.6. The UAE has demonstrated a robust commitment to combating financial crimes by issuing multiple Federal Decrees over the years to regulate AML and CFT. These laws provide a comprehensive framework to identify, assess, and mitigate financial crime risks, ensuring alignment with international standards such as those set by FATF.

5.7. The decrees emphasize stringent compliance measures, enhanced due diligence, and the adoption of risk-based approaches by financial institutions, designated non-financial businesses, and professions (DNFBPs). This proactive legislative evolution underscores the UAE's dedication to fostering transparency and safeguarding the integrity of its financial system. The Federal Decree issued by UAE are as follows:

- Federal Decree-Law No. (20) Of 2018 On 'Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations'.
- 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.
- Federal Decree Law No. (7) of 2024 amending some provisions of Federal Decree Law No. (20) of 2018
- Federal Law No. 7 of 2014 on Combating Terrorism Offences.
- Federal Law No. 5 of 2012 on Combating Cyber Crimes.
- Federal Penal Law No. 3 of 1987 (as amended), the Penal Code.
- Federal Penal Procedures Law No. 35/1992 (as amended), the Penal Procedures law.

Cabinet Decisions/Resolutions, Ministerial Decisions and Circulars

5.8. In addition to Federal Decrees, the UAE has bolstered its AML/CFT framework through a series of Cabinet Resolutions and decisions. These resolutions provide detailed guidance and mechanisms for implementing the broader legislative provisions, addressing key areas such as customer due diligence, suspicious transaction reporting, targeted financial sanctions, and governance structures for compliance.

5.9. Such Decisions/Resolutions also establish the roles and responsibilities of regulatory bodies, enhance inter-agency cooperation, and define penalties for non-compliance. Together, these Cabinet Resolutions and decisions reflect the UAE's dynamic approach to adapting its regulatory environment to emerging financial crime threats. The Cabinet Decisions/Resolutions, Ministerial Decisions and Circulars are as follows:

- 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 Financing of Illegal Organisations'.
- 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 Organisations
- Cabinet Decision No (109) of 2023 regarding regulating the procedures of the beneficial owner.
- Cabinet Decision No (132) of 2023 regarding the administrative penalties imposed on violators.
- Cabinet Decision No (74) Of 2020 On 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. (the "TFS Law")
- Cabinet Resolution No. (16) of 2021 regarding the unified list of 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.
- Ministerial Decree No. (68) of 2024 Regarding Gold Refineries' adherence to the Policy of Due Diligence Regulations for Responsible Souring of Gold.
- Ministerial Decision No. (532) of 2019 regarding the establishment of the Anti-Money Laundering Department 2019
- Ministerial Decision No. 533 of 2019 regarding the procedures for combating money.
- laundering and financing of terrorism for lawyers, notaries, and professionals.
- Ministerial Decision No. 534/2019 on the establishment of the Committee for the management of frozen, seized, and confiscated assets.
- Ministerial Decision No. 535/2019 on the procedures for the Authorisation application presented by those designated on terrorist lists to use a part of frozen assets.

- Ministerial Decision No. 536/2019 on the mechanism of grievance against the decisions issued regarding listing on local terrorist lists.
- Ministerial Decision No. 563/2019 on the procedures and conditions of the applications for international judicial cooperation in the distribution of the proceeds of crime.
- Circular No. 02 of 2021 issued by Ministry of Economy United Arab Emirates.
- Circular No. 09 of 2021 regarding GoAML reporting requirements regarding filing Dealers in Precious Metals & Stones Reporting.
- Circular No. 09 of 2021 regarding updating the list of high-risk countries\ Jurisdictions that are subject to a call for action, the list of countries that are subject to strict monitoring and updating the countermeasures that must be applied by DNFBPs.
- Circular No. 01 of 2022 regarding the results of the United Arab Emirates Money Laundering & Terrorist Financing Risk Assessment.
- Circular No. 02 of 2022 regarding Implementation of TFS on UNSCRs 1718 (2006) and 2231 (2015)
- Circular No. 03 of 2022 regarding Update the list of High-Risk Jurisdictions subject to a Call for Action and list of Jurisdictions under Increased Monitoring
- Circular No. 06 of 2022 regarding updating the list of High-Risk Jurisdictions subject to a Call for Action and list of Jurisdictions under Increased Monitoring and update the countermeasures to be applied by Designated Non-Financial Business & Professions.
- Circular No. 04 of 2022 regarding interpretative note on Assessing Jurisdictional Risk and the Consequential Application of AML/CFT Obligations considering the United Arab Emirates being among the jurisdictions under increased monitoring by the FATF.
- Circular No. (2) of 2023 Data Disclosure Notice FOR Dealers in precious metal and stone.
- Circular No. (4) of 2024 on updating the list of High-Risk Countries / Jurisdictions subject to a Call for Action, and list of Countries / Jurisdictions under Increased Monitoring, and updating the countermeasures to be applied by Designated Non-Financial Business & Professions (DNFBPs)
- Circular No. (3) of 2024 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)
- 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.
- Circular Number (3) of 2023 regarding Updated list of High-Risk Jurisdictions
- Circular No. (1) of 2023 update the list of high-risk Jurisdictions
- Circular Number (4) of 2023 on Updating the list of High-Risk Countries

- Regulation No. 1/2019 regarding declaration of currencies, negotiable bearer financial instruments, precious metals & precious stones in possession of travelers entering or leaving the UAE (issued by the UAE Central Bank on 14/1/2019 pursuant to Article 8 of Federal Law No. 20/2018).
- Central Bank Board of Directors' Decision No. 59/4/219 regarding procedures for AML and CTF and Illicit Organisations.
- Guidelines for Financial Institutions on Anti-Money laundering and combating the financing of terrorism and illegal Organisations issued by the UAE Central Bank on 23.06.2019.

International Legislative and Regulatory Framework

5.10. The fight against money laundering and the financing of terrorism is of paramount importance for international security, the integrity of the financial system, and sustainable economic growth. Recognizing the gravity of these threats, the international community has taken decisive action on multiple fronts, which includes the establishment of various Organisations that serve as global standard setters in this domain. These Organisations play a crucial role in setting international standards and best practices to combat money laundering and terrorist financing, thereby promoting a coordinated and effective response worldwide. Their efforts contribute to fostering a secure and transparent global financial environment that supports legitimate economic activities while deterring and disrupting illicit financial flows.

5.11. The AML/CFT legislative and regulatory framework in the UAE is an integral part of a broader international framework that addresses AML/CFT. This international framework consists of intergovernmental legislative bodies and international and regional regulatory Organisations.

5.12. International treaties and conventions focused on combating money laundering, terrorist financing, and preventing the proliferation of weapons of mass destruction serve as the foundation for the creation of laws at the international level. Participating in member countries then incorporate these international laws into their respective national legal frameworks.

5.13. In tandem with intergovernmental legislative bodies, international and regional regulatory Organisations play a crucial role in developing policies and recommending, assessing, and monitoring the implementation of international regulatory standards related to AML/CFT. These Organisations work to ensure consistent adherence to best practices and standards across participating member countries.

5.14. Together, these intergovernmental legislative bodies and international/regional regulatory Organisations collaborate to establish a comprehensive and harmonized global approach to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

5.15. Within the international AML/CFT framework, the government and Competent Authorities of the UAE actively collaborate with several major intergovernmental legislative bodies and international/regional regulatory Organisations. Some of these Organisations include:

- **Financial Action Task Force (FATF):** The UAE collaborates with FATF, which is the leading intergovernmental body responsible for setting global standards and promoting effective implementation of measures to combat money laundering, terrorist financing, and other related threats.
- **Egmont Group:** The UAE is a member of the Egmont Group, an international network of financial intelligence units (FIUs) that facilitates cooperation and information sharing among its members to combat money laundering and terrorist financing.
- **United Nations (UN):** The UAE works closely with the UN in implementing international treaties and conventions related to AML/CFT, including those focused on countering the financing of terrorism and the prevention of the proliferation of weapons of mass destruction.
- **International Monetary Fund (IMF):** The UAE engages with the IMF, which provides guidance and assistance to countries in developing robust AML/CFT frameworks and conducting assessments of their compliance with international standards.
- **Middle East and North Africa Financial Action Task Force (MENAFATF):** As a member of MENAFATF, the UAE collaborates with this regional Organisation that aims to enhance AML/CFT efforts and cooperation among its member countries in the Middle East and North Africa region.

5.16. These are just a few examples of the intergovernmental and international/regional Organisations with which the UAE actively cooperates in the realm of the international AML/CFT framework. Collaboration with these entities helps the UAE to align its efforts with global best practices and standards in combating money laundering and terrorist financing.

6. DEFINITION OF PRECIOUS METALS AND STONES (PMS)

6.1. Definitions of precious metals and precious stones may vary somewhat depending on region. Mostly accepted classifications internationally, based the quality, intrinsic value, and rarity, consider the precious metals to consist of gold, silver, and the so-called platinoid metals (principally platinum and palladium); and precious stones to consist of diamonds, emeralds, rubies, and sapphire. Pearls are often also included in the category of precious stones and are thus included in the supplemental guidance issued by the Regulator.

6.2. These generally accepted classifications are reflected in the federal legislation of the UAE, which governs the control, stamping and identification of PMS, as well as the import and export requirements concerning raw diamonds under the internationally accepted Kimberley Process Certification Scheme. The Broad definitions of precious metals and precious stones considered in the supplemental guidance include, but are not limited for Materials falling under the following categories:

PRECIOUS METALS

- Gold, with a minimum purity of 500 parts per 1,000;
- Silver, with a minimum purity of 800 parts per 1,000;
- Platinum, with a minimum purity of 850 parts per 1,000;

- Palladium, with a minimum purity of 500 parts per 1,000.

PRECIOUS STONES

- Diamonds (rough) of any weight in carats;
- Diamonds (polished), with a minimum weight of 0.3 carats per stone if loose, or a minimum weight of 0.5 carats per any single stone mounted in a setting (whether of one or more stones);
- Colored Gemstones (polished Emeralds, Rubies, Sapphires), with a minimum weight of 1 carat per stone if loose, or a minimum weight of 2 carats per any single stone mounted in a setting (whether of one or more stones).
- Pearls
- Loose, with a minimum diameter of 3 millimeters per bead;
- Strung or mounted in a setting (whether of one or more beads), with a minimum diameter of 10 millimeters per single bead.

OTHERS

- The above definitions notwithstanding, for the purpose of applying AML/CFT measures in respect of covered transactions, PMS to include any object concerning which at least 50 percent of its monetary value is comprised of PMS.
- Furthermore, it should also be recognized that DPMS may engage in transactions involving other types of metals and gemstones (whether traded regularly or occasionally, and whether physically or through electronic or virtual exchanges) which, while technically not considered to be PMS (although they may be of high value in some cases), may nevertheless be subject to risks of ML/FT or other predicate offences (e.g., fraud) similar to PMS. Such materials may include:
  - A variety of high-value industrial metals, including so-called conflict minerals (for example, wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g., rhodium, etc.);
  - A variety of semi-precious gemstones (e.g., amethysts, opals, jade, and others);
  - Synthetic, treated, or artificial gemstones (diamonds, emeralds, rubies, sapphires, pearls).

7. ASHKENAZI TRADING SERVICES

7.1. Established in 2023 in Dubai, Ashkenazi Trading LLC is a customer-focused company dedicated to providing exceptional services of the highest quality. With its commitment to delivering reliable and trustworthy trading solutions, Ashkenazi Trading has swiftly earned a strong reputation in the UAE.

7.2. Ashkenazi Trading a Non-Manufactured Precious Metal Trading Company & Jewellery Trading registered with DMCC bearing license number DMCC-892596. The licensed activities as per Trade License are Non-Manufactured Precious Metal Trading Company.

8. GOVERNANCE OF RISK

8.1. To effectively manage and mitigate the risks associated with AML/CFT, our Company will establish three lines of defense within its AML/CFT program. However, since the Company currently has only a small number of customers, the responsibilities for operations, compliance, and internal audit are carried out by the company's Compliance Officer.

8.2. Operations - This represents the first line of defense. As the frontline function for Know Your Customer (KYC) and Customer Due Diligence (CDD), our Company will handle customer onboarding, identification, and conduct due diligence processes. These processes involve collecting and analyzing extensive amounts of data, often obtained through comprehensive customer questionnaires and investigations.

8.3. Compliance - This serves as the second line of defense. The owner/Compliance Officer of the company will develop policies and procedures, create customer questionnaires and requirements, and maintain the necessary technologies to streamline KYC and CDD processes. If necessary, the company may engage specialist consultants to design AML/CFT policies and procedures and provide training to ensure a thorough understanding of the regulatory framework and required processes. our Company will also establish criteria for categorizing clients based on risk levels and monitor any suspicious transactions.

8.4. Internal Audit - This constitutes the third line of defense. This independent function provides assurance by assessing whether appropriate controls have been established. our Company may engage an independent compliance internal audit reviewer to conduct periodic reviews, ensuring that KYC and CDD programs are based on accurate and complete information and that approved protocols are followed during customer onboarding and transaction execution. If any deficiencies are identified, they will be reported to management, and a remediation action plan will be developed.

8.5. By implementing these three lines of defense, our Company aims to establish robust AML/CFT measures to identify and mitigate risks associated with money laundering and terrorist financing.

9. STATUTORY PROHIBITIONS

9.1. The Company affirms its commitment to comply with statutory obligations and shall not:

- Establish or maintain any Customer or Business Relationship, or conduct financial or commercial transactions, with any natural or legal person who is anonymous, identified by a fictitious name, pseudonym, or number.
- Initiate or maintain a Business Relationship or execute any transaction if unable to complete adequate risk-based Customer Due Diligence (CDD) measures for any reason.
- Engage with Customers listed on any sanctions watchlist, the United Nations “Consolidated List,” or the UAE Local Terrorist List.
- Use professional or contractual confidentiality as a justification for failing to fulfill statutory reporting obligations concerning suspicious activities.

10. ROLES AND RESPONSIBILITIES

10.1. Board of Directors: The Board of Directors are committed to setting the highest standards of Compliance and Governance. The key roles and responsibilities of the BOD has been outlined below:

- BOD should approve a robust and effective AML CFT Compliance and Governance Framework which has complete independence in performing job objectives.
- Approve AML CFT policy, related procedures, ML/FT risk assessment framework and onboarding risk assessment methodology and controls to mitigate the risks including amendments.
- Approve the appointment of a qualified MLRO with the necessary industry experience & certification required and approved by the Regulator.
- Approve Enterprise-wide ML/FT Annual Risk Assessment report.
- Approve ML/FT Risk Appetite Statement (including related updates).
- Ensure a robust and effective independent audit function is in place.

10.2. Compliance Officer:

- Ensure that appropriate policies, procedures, systems, and controls are established, developed, and maintained to monitor day-today operations for compliance with AML law, regulations, policies, procedures, systems, and controls.
- Conduct regular gap analysis on new notices/regulations/best practices issued by regulatory bodies vis-à-vis this AML & CFT Compliance policy.
- Conducting Enterprise-Wide AML/CFT Risk Assessment (at least on an annual basis).
- Conducting AML/CFT Risk Assessment of any new and/or modified product, service, and delivery channel
- Ensure adequacy of the systems and measures of customer due diligence and reasonability and creditability of the customer information obtained to establish a Business Relationship or carry out a transaction;
- Review high risk customers and ensure enhanced ongoing due diligence is undertaken for all high-risk customers / clients;
- Ensure to have in place a process for monitoring transactions for potential suspicion and reporting suspicious transactions;
- Control the level of the Company's compliance with the development of systems and procedures that ensure updating the records, and the extent to which such systems and procedures are applied on a regular basis;
- Ensure all key documents pertaining to KYC of customers, customer transactions, trainings and STR are retained for the minimum period of five (05) years.
- Arrange for AML/CFT training for all the employees; monitoring appropriateness and effectiveness of the AML/CFT training programs.

- Oversight on the implementation of AML policies, procedures, systems, and controls, including the risk-based approach to ML/FT risks.
- Filing STRs to the FIU, immediately once a suspicion is confirmed or maximum within two working days after completion of necessary investigation.
- Acting as focal or central point of contact between the FIU, the Regulator(s), and State authorities in relation to AML issues.
- Ensure prompt response to request for information by the FIU, Regulator(s), and State authorities in relation to AML issues.
- Producing bi-annual reports on the effectiveness of the AML / CFT controls, for consideration by senior management and Board.
- Exercising all other functions given to CO under AML/CFT Law, regulations or on issues relating to AML/CFT including accessing the GoAML portal of the FIU and filing STR and other reports to them.
- The CO must execute his responsibilities honestly, reasonably, and independently, particularly while receiving, investigating, and assessing internal STRs.
- Ensure that the Company sets the disciplinary regulations and procedures that ensure the commitment of that Company's employees to implementing the provisions of this policy

11. RISK FACTORS RELATING TO ASHKENAZI TRADING

11.1. The precious metals and stones sector offers opportunities for criminals seeking to conceal, transfer, and/ or invest their illicit proceeds. Precious metals and stones offer high value by weight, are difficult to trace and identify, and retain their value over time. Dealers in precious metals and stones (DPMS), if they do not apply effective preventive measures, could be vulnerable to abuse by illicit actors engaged in laundering the proceeds of crime, financing terrorism, arms trafficking, and sanctions evasion.

11.2. The characteristics of precious metals and stones make them uniquely appropriate as a medium to store, transfer, and exchange value:

- Precious metals and stones are generally compact, durable, odorless, and of high value.
- Certain metals/stones (e.g., gold/diamond) are widely accepted as a method of exchange or currency.
- Precious metals/stones retain their value over time and have roughly similar value all over the world.

11.3. In addition to these properties, precious metals and stones have characteristics that make them particularly attractive to criminals seeking to launder funds and others engaged in illicit behavior:

- Differentiating precious metals and stones often requires laboratory techniques, so it can be difficult or impossible to track their movement.

- Precious metals and stones can be transformed (through re-cutting or recycling) into different objects while retaining their value, interrupting known custody and transfer chains.
- Purchase, sale, and exchange of precious metals often take place outside the formal financial system.

11.4. For these reasons, DPMS may be targeted by illicit actors seeking to abuse their services and exploit the advantages of precious metals and stones. Although most transactions involving DPMS are legal, these businesses may trade in items that could be the proceeds of crime, purchased with the proceeds of crime, and/or used to launder the proceeds of crime, unknowingly or complicitly.

11.5. Complicit DPMS may knowingly partake in illicit activities and may in turn use their business relationships with our Company to launder the proceeds of crime or carry out other illicit activity. Even DPMS that are not knowingly involved in illicit activities may use their accounts with our Company to deal in the proceeds of crime.

Features of DPMS that Increase Risk

11.6. Not all DPMS pose equal risks. A DPMS is likely to be considered a higher risk when it provides products or services that are attractive to illicit actors, has operations in high-risk jurisdictions including conflict-affected and high-risk areas (CAHRAs), or does not apply appropriate AML/CFT controls.

Regulatory Environment

11.7. In many jurisdictions, DPMS are not required to comply with requirements related to identification of customers and reporting suspicious activities. In other jurisdictions, these requirements are nominal.

11.8. Various DPMS are not subject to effective supervision and enforcement. Even in a jurisdiction that imposes and enforces such requirements, they frequently apply only to DPMS that engage in cash transactions above a certain value threshold. Where DPMS are unregulated or under-regulated, they are unlikely to be taking effective measures to protect themselves from abuse.

11.9. In contrast, an effective AML/CFT framework and supervisory regime for DPMS can protect DPMS by effectively imposing AML/CFT requirements and by detecting, deterring, and prosecuting ML/TF crimes. It is important to note that certain DPMS in the UAE are required to comply with all requirements of AML-CFT Decision, including the requirement to perform Customer Due Diligence (CDD) and report suspicious transactions.

Products, Services, and Delivery Channels

11.10. Products, services, and delivery channels that facilitate the rapid, efficient, anonymous movement of value on a large scale will be more attractive to illicit actors and may put a DPMS at a higher risk of abuse. Such products, services, and delivery channels may include:

- Products (such as bullion and uncut stones) that are particularly hard to trace, retain or even increase in value despite being transformed into new forms (melted down, re-cut, etc.), and offer high value by weight.
- Services, such as metal accounts, allow customers to rapidly purchase and sell precious metals.

- Delivery channels that allow transactions to be carried out quickly and anonymously, such as accepting cash or virtual assets and conducting transactions online or through intermediaries.

Customer Base

11.11. The types of customers that a DPMS serves can also impact risk. For example, a DPMS that primarily deals with PEPs may be a higher risk than one that serves a lower-profile clientele.

Geography

11.12. DPMS may be based, or may trade internationally, in jurisdictions that are of higher risks for money laundering, the financing of terrorism, and the financing of proliferation. Such DPMS may pose heightened risk to Licensed Financial Institutions (LFIs). Higher-risk jurisdictions including CAHRA may be characterized by:

- A low level of government oversight and regulation of the precious metal and stone value chain.
- Low economic and political stability.
- High use of the informal banking system.
- High levels of corruption.
- The presence of terrorist and other non-state armed groups.
- Weak border control measures; and/or
- Sanctions and embargoes

12. ML/TF RISKS

12.1. When required to apply AML/CFT measures, our Company should carefully consider factors such as customer risk, geographic risk, channel risk, products, services, and transactions risks. Consideration should be given to such factors as:

- Counterparty/customer type, complexity and transparency (e.g. whether the counterparty or customer is a physical person, a legal person or a legal arrangement; if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a 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.
- 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; 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).
- 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) is associated with a High-Risk Country,

particularly in relation to locations where the transactions are conducted, and the goods are delivered.

- 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).
- Type, nature, and characteristics of the products and/or services, including but not limited to quantity, quality/level of purity, price/value, form (physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity.
- Type, size, complexity, cost, and transparency of both the transaction (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, local market practices, and the degree of expertise required.
- 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.

13. CASH POLICY

13.1. Our Company recognizes the significance of handling cash and maintaining records to comply with regulations and ensure transparency in its operations. To adhere to the requirements of the Ministry of Economy, specifically Circular No. 08/AML/2021 dated 02 June 2021, our Company actively reports cash transactions. Additionally, our Company has implemented strict procedures to accurately document cash receipts and report specified transactions.

13.2. Our Company ensures the proper reporting of all cash transactions as specified by the Ministry of Economy in accordance with the Circular. This involves recording essential details such as transaction amount, date, customer information, and any other required particulars.

13.3. Our Company maintains comprehensive documentation for all cash transactions, which includes issuing receipts or invoices to customers. These documents precisely capture transaction details such as the goods or services provided, payment amount, and any other relevant information.

14. CUSTOMER ACCEPTANCE POLICY

14.1. The Company shall follow the customer acceptance policy and procedures, in accordance with national and international regulations and best practices, to prevent the commencement of business relationships with customers against whom sanctions or restrictions have been imposed, or with customers who pose a non-acceptable level of risk to the company and its business operations.

14.2. The Company will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate and shall establish AML/CFT procedures to assist and guide

employees in carrying out their responsibilities and ensure that ML/FT risks are taken into consideration in the company's daily operations.

Natural and Legal Person/Entity

14.3. The Company will establish the identity of its clients and beneficial owners prior to establishing business relationships with such persons and will take reasonable measures to verify identity when establishing a business relationship as noted below, subject to applicable EOCN requirements.

- **Natural Persons:** Identity will be verified to the company's satisfaction based on official identity papers or other reliable, independent source documents, data, or information as may be appropriate under the circumstances as per the procedures mentioned in Know Your Customer (KYC) section of this Policy.
- **Corporations, Partnerships & other Legal Entities:** Identity will be verified based on documentary evidence of due organization and existence as per the procedures mentioned in Know Your Customer (KYC) section of this Policy.

Ultimate Beneficial Owner

14.4. The Company will ensure to identify the identity of each beneficial owner who will be established and verified unless the identity is previously verified in accordance with the beneficial owner's role as a client. Identity will be verified to the Company's satisfaction based on officially valid identity papers or other reliable, independent source documents, data, or information as may be appropriate and in the event verification, copies of such documents will be obtained.

Politically Exposed Persons

14.5. The Company shall only enter a business relation with a PEP (natural person or legal person/ arrangements) upon gaining approval from the CO and the Owner during the onboarding phase. The Company will also ensure that the customer, whether a natural person or a legal entity, is frequently monitored during the period of relationship.

14.6. Any declassification of PEP should be subject to an appropriate level of senior management review and approval. This review should be documented. Once a PEP has been de-classified, their prior PEP status should be noted for investigatory purposes (e.g., in the event of a suspicious activity reporting).

High Risk Jurisdiction Customers

14.7. The Company will ensure to undertake EDD process that is effective and proportionate to the ML/FT risks, including obtaining the approval of the CO, for establishing business relationships or one-off transactions with Customers from high-risk jurisdictions which include conflict-affected and high-risk areas as per the procedures mentioned in this Policy.

Others

14.8. The Company will ensure to undertake EDD process that is effective and proportionate to the ML/FT risks, including obtaining the approval of the CO and the Owner (if necessary), for establishing business relationships with third parties, NPO's or one-off transactions with Customers who conduct

unusually complex transactions or those which have no clear economic or legal purpose and make sure to frequently monitor transactions processed by these customers and report to FIU in case of any suspiciousness.

15. PROHIBITED CUSTOMER TYPES/ BUSINESS RELATIONSHIPS

15.1. The Company has categorized various kinds of clients whose commercial dealings call for increased levels of due diligence. This will often be the case in situations in which the company's business activities are anticipated to present a risk that is greater than the company's average risk. Transactions involving restricted customer categories are a type of ML/FT typology that is frequently employed by organizations that participate in the criminal underworld and professional money launderers.

15.2. The following are the conditions under which Ashkenazi Trading will refuse to accept a new business connection or will end an existing one. The following are some examples of such circumstances:

- Persons (natural or legal) who are unable to meet the company's identification and verification requirements or existing customers who no longer fulfill them.
- Shell banks / company
- Persons (natural or legal) or existing customers on sanction lists or lists provided by the EOCN or other regulatory authorities.
- Customers for whom suspicious transaction reports have been repeatedly submitted to the FIU, unless the latter requests the accounts to remain open so as to facilitate the investigation process.

15.3. Prohibited transactions, these are transactions for which the company has assessed that the level of risk is not acceptable to the Company.

16. DUE DILIGENCE

16.1. The Company ensures that required CDD measures are undertaken to verify the identity of the Customer and the Beneficial Owner either before or during the establishment of a business relationship, or prior to executing a transaction for a Customer with whom there is no existing business relationship.

16.2. In cases where the crime risk is assessed to be low, the Company may complete the verification of the Customer's identity after the establishment of the business relationship, subject to the following conditions:

- Verification will be conducted promptly following the commencement of the business relationship or execution of the transaction.
- Any delay in verification is necessary to avoid obstructing the natural course of business.
- Appropriate and effective measures will be implemented to manage and mitigate the risks of financial crime.

- The Company will implement requisite risk management measures to address scenarios where Customers may benefit from the business relationship before the completion of the verification process.

17. CUSTOMER DUE DILIGENCE (CDD)

17.1. Customer Due Diligence (CDD) is the process of identifying and verifying the customer's identity, understanding nature of business activities and establish purpose of business relationship before carrying out a transaction and/or establishing business relationship with customer. An adequate CDD / KYC process ensures that the Company deals with legitimate customers and prevents any possibility of financial crime risks.

17.2. Customer Due Diligence measures must be applied in the following cases:

- Before establishing a business relationship
- Before carrying out a transaction for a customer with whom it does not have an established business relationship which value is equal to or greater than AED 55,000 for transactions carried out in a single transaction or multiple inter-related transactions.
- When there is a suspicion of money laundering or terrorism financing.

17.3. When there are doubts concerning the veracity or adequacy of previously obtained identification documents and information

18. CUSTOMER DUE DILIGENCE MEASURES

18.1. The Company ensures robust Customer Due Diligence measures, including but not limited to the following:

- **Customer Identification and Verification**: Identifying and verifying the Customer's identity using reliable, independent source documents, data, and information issued by public authorities.
- **Beneficial Ownership Verification**: Identifying and verifying the Beneficial Owners associated with the business relationship or transactions.
- **Authorized Representatives**: Identifying and verifying the identity of any individual acting on behalf of the Customer, including authenticating their authority to do so.
- **Legal Arrangements**: Identifying and verifying the following roles in legal arrangements:
  - Trustees, managers, directors, or equivalent persons.
  - Settlers, founders, or equivalent persons.
  - Entities settling assets into trust or legal arrangement.
  - Protectors or equivalent persons exercising ultimate control.
  - Beneficiaries or equivalent persons.
  - Signatories are associated with the legal arrangement.

- **Nature of Business Activities**: Understanding the Customer's business activities to ensure that the funds involved in transactions are from legitimate sources.
- **Purpose and Intended Nature**: Gathering specific information or conducting specific measures to understand the purpose and intended nature of the business relationship, or inferring the same from the type of transactions or relationship established.
- **Background Screening**: Conducting background checks on the Customer, Beneficial Owners, beneficiaries, or controlling persons to identify:
    - Applicability of targeted or international financial sanctions.
    - Potential adverse information, such as criminal history, particularly in higher-risk scenarios.
- **Ongoing Monitoring**: Supervising and monitoring the business relationship to ensure consistency between conducted transactions or activities and the information gathered about the Customer and their expected behavior.

19. CDD FOR INDIVIDUALS (IDENTIFICATION AND MEASURES)

Customer Identification for Transaction below AED 55,000

19.1. It is the policy of the Company to identify customer/beneficial owner information for executing any transaction below AED 55,000. The following information must be identified for an individual customer:

- Name of the customer
- Nationality
- Date of Birth (DOB)
- Mobile Number
- Valid ID number
- ID Issue and Expiry Date

Customer Verification for Transactions below AED 55,000

19.2. A valid Identification document must be collected from the customer to verify above information.

19.3. Valid Identification document for individuals is:

- Emirates ID for residents
- Passport with valid visa for non-resident
- GCC identity card for GCC citizens

Customer Identification and Verification for Transactions above AED 55,000

19.4. Customer Identification

- Know Your Customer Form (Refer to KYC form for Individual)

- The minimum information to be obtained includes Name, Nationality, Date & Place of Birth, Occupation, Identification Number, Permanent Residential Address, Occupation, Employer Name and Employer Address.
- Nature and Purpose of Business Relationship
- Customer Verification
- Emirates ID for Emirati nationals and non-Emirati residents
- Passport and Valid Visa for non-residents
- GCC ID Card for GCC Citizens
- Address proof such as official documents, utility bills, tax assessments, bank statements, insurance policies, or a letter from a public authority.
- The documents are required to be verified with original by the Company staff or apostille seal if country of issue is member of Hague Convention or concerned foreign embassy attestation (if not member of the Hague Convention).

20. CDD FOR LEGAL ENTITIES (IDENTIFICATION AND VERIFICATION MEASURES)

20.1. To apply CDD measures on Legal persons/ arrangements, below mentioned valid and official documents are collected:

- Know Your Customer Form (Refer to KYC form for Corporate)
- Minimum Legal Entity/Arrangement information such as Name, Legal Form, Registered Address, nature of business activities, ownership and/or control structure, Date and Place of Incorporation, Nature and Purpose of Relationship with the Company, Trade License / Commercial Registration Number, Identification details of shareholders, ultimate beneficial owner, authorized signatories, and senior management members etc.
- Commercial license issued by the Ministry of Commerce and Industry (for resident companies and establishments);
- For legal arrangements such as charities, trusts, etc., official identification documents attested by competent public authorities or bodies that issue these documents.
- In the case of non-resident companies and establishments, documents issued by competent authorities in the state in which they were incorporated or established.
- Identification documents of Ultimate Beneficial Owner or Controlling persons in case of legal arrangements.
- Authorization letter or Power of Attorney for Authorized Signatory/ Representative.
- Identification document of Authorized Signatory/Representative.
- Memorandum and Articles of Association.
- Address proof such as official document, utility bills, tax assessments, bank statements, or a letter from public authority.

Identification of Ultimate Beneficial Owner

20.2. In case of legal person / arrangement, the Company identifies:

- The natural persons who ultimately have a controlling ownership interest of more than 25% either by shares or by voting rights in a legal person; or
- If there is doubt as to whether the persons with controlling ownership interest are indeed the beneficial owners, or where no natural person exerts control through ownership interests, the natural persons exercising control of the legal person through other means; or
- In the exceptional circumstances of an absence of any natural persons who have controlling ownership or otherwise exercise effective control of the legal person, the natural person who holds the position of senior managing official.
- The Beneficial Owners may be verified by obtaining the Beneficial Information filed by the Legal Entity to the Registrar.
- The documents are required to be verified with original by the Company staff or apostille seal if country of issue is member of Hague Convention or concerned foreign embassy attestation (if not member of the Hague Convention).

21. EXEMPTION TO CUSTOMER DUE DILIGENCE

21.1. The Company shall be exempted from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner, if such information is obtainable from reliable sources where the Customer or the owner holding the controlling interest are as follow:

- A company listed on a regulated stock exchange subject to disclosure requirements through any means that require adequate transparency requirements for the Beneficial Owner.
- A subsidiary whose majority shares or stocks are held by the shareholders of a holding company.

21.2. The listed Company (as defined above) should be subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In such case, the DPMS will obtain customer identification information from the stock exchange website, where it is listed.

22. ENHANCED DUE DILIGENCE (EDD)

22.1. The Company shall implement Enhanced Due Diligence measures in certain scenarios based on the high-risk factors.

22.2. The Risk factors can be categorized into four key areas:

- Customer Type Risk (such as Non-Resident Customers, Customer involved with high-risk business activities, nonprofit organizations, PEP)
- Geography Risk (customers associated with or conducting transactions through High-Risk Countries)
- Product / Services/ Channel Risk (High risk products such as bullion trading / gold exchange/extraction/ refining etc.).

- Transaction Risk (cash, high value, and international transactions) - (Please refer to ANNEXURE II- High Risk Factors)

23. EDD MEASURES

23.1. EDD involves a more rigorous application of customer due diligence measures to be applied for high-risk business relationship. EDD measures may include, but not limited to:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources regarding customer identity.
- More detailed inquiry and evaluation of reasonableness about the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of each transaction.
- Perform adverse media checks on customers and/or beneficial owners to identify any involvement of financial crime.
- Update more regularly the information on customers and beneficial owners (at least annually).
- Obtain the approval of senior management to commence or continue the business relationship.
- Conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Payment is to be carried out through an account in the customer's name with a financial institution subject to similar customer due diligence standards.
- Establish source of funds and purpose of transaction, if required obtain evidence also.

24. SIMPLIFIED DUE DILIGENCE

24.1. Ashkenazi Trading under certain circumstances and in the absence of a ML/FT suspicion, is permitted to exercise simplified customer due diligence measures (SD) regarding customers identified as low risk through an adequate analysis of risks.

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

- A reduction in verification requirements regarding customer or Beneficial Owner identification.
- Fewer and less detailed inquiries regarding the purpose of the Business Relationship
- More limited supervision Of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information,

24.3. As per the AML Decision, SDD can be done in the following cases:

- Identified low-risk customers
- Listed Companies

25. SUPPLIER DUE DILIGENCE

25.1. Performing due diligence procedures on Suppliers reassures that the potential suppliers are financially and legally sound thus reducing the company's risk of exposure. The Company must ensure that all the necessary information required to assess the supplier must be collected.

25.2. Suppliers could either be outsourced for various products or services or could be third parties that provide essential commodities/ services. The SDD approach must be flexible and must emphasize the main risk areas that the company is likely to be exposed to.

26. SUPPLIER DUE DILIGENCE MEASURES

26.1. Supplier Due Diligence involves (but not limited to) the following processes:

- Identifying and assessing supplier specific risks relative to the industry it operates in;
- Screening for third party relationships of the supplier and therefore the regulatory environment.
- Identifying and screening third party connections which can expose the supplier to a greater risk of money laundering;
- Screening for any negative news that is against the supplier;
- Risk Assessment must be conducted with all (trade related) suppliers and those classified as High Risk will be subject to Enhanced Due Diligence.

26.2. As part of the Due Diligence process, vendors must be requested to fill in a Know Your Supplier form prior to onboarding the supplier or executing transactions.

27. EMPOLYEE DUE DILIGENCE MEASURES

27.1. When hiring employees, directors, board members and executive or supervisory management shall establish screening procedures to ensure that:

- Employees, directors, board members and executive or supervisory management, CO(s) and internal auditors have the high level of competence necessary for performing their duties;
- Employees, directors, board members and executive or supervisory management, CO(s) and internal auditor(s) have appropriate ability and integrity to conduct the business activities of the Company;
- Potential conflicts of interest are considered, including the financial background of the employees, directors, board members, executive or supervisory management, CO(s) and internal auditor(s); and
- Persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the Company.

28. EMPLOYEE SCREENING

28.1. The screening procedures must include the following at a minimum:

- Initial screening of CVs.
- Verification of applicants' academic qualifications.

- Testing and interview.
- Employment history verification by contacting previous employers to confirm the employee's work experience and to gather information on previous role(s).
- Sanction checks must be applied to applicants before placing them in employment.

29. POLITICALLY EXPOSED PERSONS (PEP)

29.1. PEP is an acronym for Politically Exposed Persons. PEPs are persons with political power who can exercise political influence to carry out business activities and other administrative roles at their discretion. PEPs are most likely to be suspected of bribery and involved in corrupt activities, as they influence the spending of government funds. It is noteworthy that not only the person with political power but also the family, friends, and close associates are also considered high-risk customers owing to the relationship they share with the PEP.

29.2. PEP's definition may differ from country to country, and it's a broad term in which businesses exercise their best judgment to identify a PEP. There are several factors that businesses need to consider in the risk assessment, such as the type of business, the country in which it operates, and the local AML regulations.

29.3. Identifying a Politically Exposed Person (PEP) can be a challenging task. The customer identification process is crucial as the exercise can help a business correctly assess the risk of creating a business relationship with PEP. If the identity and connections of the person are not known to the company and without correct risk assessment, mitigation of the risk becomes complex leading to reputational damage.

30. CATEGORIZATION OF PEP

30.1. The definition of PEP differs from one country to another. People working in the government at different levels are described as PEPs:

- Members of Parliament, Heads of state – presidents, ministers, heads of departments, mayors, etc. can be categorized as PEP.
- People at the judicial levels, such as judges, are also classified as PEP. But not all judges fall under the PEP category.
- People holding diplomatic positions such as ambassadors and senior positions in the management of government-run organizations are also considered PEP.
- Bank officials in senior positions of national banks are regarded as PEPs.
- Senior officials in the sporting events responsible for organizing events and closing contracts on behalf of the government or ministry are also considered high-risk customers and fall under the PEP category.
- Parents, children, spouses, partners, siblings, and close relatives can also be called PEPs. So, they are also subject to EDD because they are associated with PEP.
- People with close business relationships with PEP are also considered persons associated with PEPs; people holding joint beneficial ownership or legal arrangements with the PEP

are considered high-risk customers. Associates who conduct transactions on behalf of the PEP are also categorized as high-risk customers. UBOs established to provide benefits to the PEP are also considered PEPs.

31. IDENTIFICATION OF PEP

31.1. Ashkenazi Trading follows a robust AML compliance framework. Through this, Ashkenazi Trading can accurately assess the risk of different customers. It helps to correctly identify and verify the customer's identity and flag the potential PEP – whether domestic PEPs, foreign PEP or HIOs.

31.2. Ashkenazi Trading relies on AML screening software which helps the company to identify and verify customers and their status as PEP or associated with PEP.

31.3. With CDD and EDD processes and continuous monitoring, the company accurately identify PEPs, monitor their status, and make transactions with them.

31.4. Ashkenazi Trading identifies the PEP at the first step of initiating the customer relationship. Also, continuous monitoring is applied, as the PEP status may change over a while.

31.5. It keeps a tab on the PEP status. It helps to assess the risk involved during the customer journey correctly. To assess the PEP status accurately, it tries to get accurate information in real-time.

31.6. PEPs are entrusted with administration responsibilities and wield power to get things done at their discretion. Therefore, Ashkenazi Trading uses EDD as a powerful method to identify the source of PEP's funds and verify their financial and professional background before becoming a PEP.

31.7. EDD will help make an informed decision regarding establishing a business relationship with people identified as PEPs – they may be close associates, family, or friends of the PEP. Continuous monitoring of the customer profile is also required to detect any changes from the original verification conducted at the time of on-boarding. Often non-profit organizations, charities, etc., are misused to launder money by the PEPs, so the company also verifies the PEPs' connection with such charitable organizations.

32. SANCTIONED INDIVIDUALS/ENTITIES

32.1. Our Company will take all the required steps to ensure that all customers with whom a business relationship is established are screened against relevant notices such as:

- United Nations sanctions (UN)
- UAE (Local Terrorist List)
- the Office of Foreign Assets Control (OFAC)
- Her Majesty's Treasury Department – UK (HMT)
- European Union sanctions (EU)

32.2. Any confirmed matches to sanctions lists will be declined for a business relationship, and the necessary reports will be made to the Financial Intelligence Unit (FIU).

32.3. Our Company shall document and record all the actions that were taken to comply with the sanction's regime and the rationale for such action. The Compliance Officer will consider if any further action is required such as freezing funds in accordance with Section 22 on TFS.

33. UPDATING KYC INFORMATION

33.1. KYC is an ongoing process. The foundation of any CDD and monitoring procedures lies in the initial collection of KYC information and the ongoing updating of that information.

33.2. KYC information is crucial for effective CDD and ongoing monitoring. Our Company recognizes the importance of maintaining accurate customer information and will take reasonable steps to ensure that KYC information and documents are updated as and when necessary.

33.3. As a minimum standard, our Company will conduct KYC information updates at least once a year for ongoing business relationships. This ensures that any changes in the customer's profile, risk factors, or regulatory requirements are captured and reflected in the customer records.

33.4. By regularly updating KYC information, our Company aims to maintain the integrity of its customer database, enhance risk assessment accuracy, and ensure compliance with applicable laws and regulations. This ongoing process helps in mitigating potential risks associated with money laundering, terrorist financing, and other illicit activities.

34. MONITORING OF CLIENT'S ACTIVITIES

34.1. In line with regulatory requirements, our Company is committed to ongoing supervision of established business relationships to ensure compliance and mitigation of risks associated with money laundering and other illicit activities. This includes conducting audits of customer transactions throughout the course of the relationship to verify their consistency with the information provided, stated activities, and risk profiles.

34.2. For customers or business relationships identified as high risk, our Company will conduct additional investigations and gather more information about the purpose of transactions they intend to conduct. Enhanced ongoing monitoring and review of transactions will be implemented to identify any potentially unusual or suspicious activities.

34.3. Considering the level of risk involved, our Company will evaluate the specific details of examined transactions in relation to the customer's due diligence, information or profile. This evaluation includes obtaining sufficient information about the counterparties and other involved parties, utilizing available public sources such as internet searches. The objective is to determine whether the transactions appear to be:

- **Normal**: They align with the typical transactions conducted by the customer, the other parties involved, and similar types of customers.
- **Reasonable**: The transactions have a clear rationale and are consistent with the typical activities engaged in by the customer and the counterparties.

- **Legitimate**: The customer and counterparties are authorized to engage in such transactions, including having any required licenses, permits, or official Authorisations.

34.4. By conducting thorough evaluations and obtaining relevant information, our Company aims to ensure that transactions are in line with regulatory requirements and to identify and prevent any potentially illicit or suspicious activities within established business relationships.

35. INDICATORS OF SUSPICIOUS ACTIVITIES - RED FLAGS

35.1. Criminals continuously adapt their methods for conducting money laundering, financing of terrorism, and financing illegal Organisations. Consequently, there may be unique characteristics within a specific market or type of trust and company services that go beyond the red flags identified in this policy. Therefore, the following list of red flag indicators for potentially suspicious transactions should not be considered exhaustive.

35.2. It is important to note that the presence of one or more of these indicators does not necessarily imply that a transaction involves money laundering or financing of terrorism. However, it suggests the need for enhanced due diligence or further investigation. This will enable our Company Owner/Manager to make appropriate determination as to whether the transaction should be regarded as suspicious or not.

35.3. Red flags should be raised regarding trade practices in the following circumstances:

- Precious metals/stones originate from a country with limited or no production of such materials.
- Conducting trade in large volumes with countries that are not part of a specific precious metals and stones pipeline.
- Noticing a significant increase in activity volume in a DPMS (Diamond, Precious Metals, and Stones) account despite a substantial decrease industry wide.
- Observing the buying or selling of precious metals and stones between two local companies through an intermediary located abroad, with a lack of business justification and uncertainty regarding the actual movement of goods between the companies.
- Encountering purchases and/or imports of precious metals and stones that greatly exceed the expected sales amount.
- Identifying the use of a single bank account by multiple businesses.

35.4. A red flag should be raised with respect to the business relationship or the customer in the following circumstances if the customer:

- Suddenly cancel a transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, raising reasonable doubt about the accuracy or sufficiency of the information provided.
- Is unwilling, unable, or refuses to explain their business activities, corporate history, identity of the beneficial owner, source of wealth/funds, reasons for conducting activities in a certain manner,

parties involved in transactions, or nature of business dealings with third parties (especially those in foreign jurisdictions).

- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or appears in reliable, publicly available information sources with adverse information such as corruption or criminal allegations.
- Is a designated person or Organisation listed on a Sanctions List.
- Is related to or associated with a person suspected or involved in terrorism or terrorist financing operations.
- Insists on using an intermediary without sufficient justification, either professional or informal.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has connections with politically exposed individuals, either through familial or professional associations.
- Is a foreign national with no significant business dealings in the country and no clear economic or other valid reasons for engaging with our Company.
- Is located a significant distance away from our Company without a logical rationale.
- Refuses to cooperate or provide necessary information, data, and documents for facilitating a transaction, or demonstrates unfamiliarity with the details of the requested transaction.
- Make unusual requests, including those related to secrecy, to our Company or its employees.
- Is willing to pay significantly higher fees without legitimate reasons.
- Appears to be overly concerned about or asks an unusual number of detailed questions regarding compliance-related matters, such as customer due diligence or transaction reporting requirements.
- Conducts a transaction that appears incompatible with their socio-economic, educational, or professional profile, or demonstrates a lack of understanding regarding the transaction.
- Utilizes legal entities, legal arrangements, or foreign private foundations operating in jurisdictions with secrecy laws.
- Requests services (e.g., smelting and reshaping of gold into ordinary-looking items) that could potentially disguise the nature of precious metals or stones or conceal beneficial ownership from authorities, without a clear legitimate purpose.
- Claims to be a legitimate entity engaged in Diamond, Precious Metals, and Stones (DPMS) activities but cannot provide evidence of real activity or a credible history.
- Cannot be found on the internet or social business network platforms, such as LinkedIn.
- Is registered under a name that does not indicate a relationship with DPMS activities or indicates different activities from those claimed.

- Utilizes an email address with a public or non-professional domain (e.g., Hotmail, Gmail, Yahoo).
- Is registered at an address that does not match the company's profile or cannot be located on internet mapping services like Google Maps.
- Is registered at an address associated with numerous other companies or legal arrangements, suggesting the use of a mailbox service.
- Has directors or controlling shareholders 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 of their Authorisation for the transaction.
- Is incorporated or established in a jurisdiction considered to pose a high risk of money laundering, terrorism financing, or corruption.
- Has a complex corporate structure that seems unnecessary or lacks commercial sense.
- Appears to be acting according to instructions from unknown or inappropriate individuals.
- Conducts an unusually high number of transactions within a relatively short time.
- Requests shortcuts, excessively quick transactions, or complicated structures that pose unnecessary business risk or expense.
- Asks for payment arrangements that are unusually or unnecessarily complex or confusing, involve third parties, or require various forms of payment.
- Provides identification, records, or documentation that appear falsified or forged.
- Requires transactions to be processed primarily or exclusively through cash, cash equivalents, or virtual currencies to preserve anonymity, without adequate and reasonable explanation.

35.5. A red flag should be raised with respect to the transaction if it:

- 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 gold) or jewellery for cash in small incremental amounts.
- Involves the barter or exchange of PMS (especially gold) or jewellery for other high-end Jewellery.
- Appears structured 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.

- Involve payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves PMS with characteristics that are unusual or do not conform to market standards.
- Involves the unexplained use of powers-of-attorney or similar arrangements to transact business on behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other authorized representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involve 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).
- 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 begins 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.

- Insist on an unusually quick completion, without a reasonable explanation.

- Takes place through intermediaries who are foreign nationals or individuals who are non-residents.
- 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).

35.6. A red flag indicator for 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 traveler's cheques, cashier's cheques and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PMS.
- The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Is divided into smaller parts or instalments with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.
- Cannot be reasonably identified with a legitimate source of funds.

36. TRAINING AND AWARENESS

36.1. In order for the ML/FT risk assessment and mitigation measures to be effective, the Company shall ensure that its employees have a clear understanding of the risks involved and can exercise sound judgment, both when adhering to the organization's ML/FT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/FT risk, the Company shall ensure that its employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks.

Employee's Training

36.2. Ashkenazi Trading has an ongoing employee training under the leadership of the Compliance Officer.

36.3. The AML/CFT training materials prepared by the Company will cover at least the following topics. These topics should be covered in greater depth, and additional topics should be covered as appropriate, on a risk sensitive basis depending on the role of each employee:

- Overview AML/CFT, definitions, typologies as well as contemporary trends.
- ML/FT risks are associated with the products and services offered.
- AML/CFT policies and procedures include the highlights of recent changes.
- The regulatory responsibilities and obligations of employees under AML/CFT Laws, Regulations, Notices, and Standards.
- Description of Know Your Customer process and its importance.
- Due Diligence measures and procedures for monitoring transactions.
- Sanction screening and PEP screening procedures.
- Red flags to identify unusual transactions or transaction patterns or customer behaviors.
- Processes and procedures of making internal disclosures of unusual transactions.
- Roles of the CO and the Senior Management.
- Awareness of Tipping off.
- Record retention policy.
- Reference to industry guidance and other sources of information.
- Emerging ML/FT risks and measures to mitigate such risks.
- Penalties for non-compliance with the AML/CFT Laws, Regulations, Notices, and the Standards; and
- Disciplinary procedures are to be applied to employees for not adhering to the AML policy and procedures.

36.4. Means of the training may include educational pamphlets, videos, internet systems, in-person lectures, and explanatory memos. The operations are reviewed periodically to see if certain employees, such as those in compliance, margin, and corporate security, require additional specialized training.

Annual Training Plan

36.5. The Ashkenazi Trading shall ensure that AML/CFT trainings are conducted at all levels within the Company (including functional heads, Senior Managements and Owner). To achieve this goal, the CO will develop an annual training plan after assessing employees' specific training needs and their respective obligations at the beginning of the year.

36.6. All employees must be trained to understand how to comply with the legal and regulatory framework in the UAE and abide by the Company's policies and procedures. It is not acceptable for an untrained employee to have responsibility for collecting or disbursing customer funds and initiating transactions.

36.7. The Company shall provide AML/CFT training as follows:

- Induction Training: All the new joiners shall be provided with AML training as soon as reasonably practicable within 30 days after joining the firm and new joiners is not allowed to serve the any customer independently until attending the training.
- Refresher Training: Refresher training shall be provided by an external party at regular intervals as per the annual training plan of the Company. The Company may determine the frequency of refresher training based on the risk exposure of the employee. However, employees who deal directly with customers, products and services will receive annual training at a minimum.
- Ad-hoc Training: Additional training will also be provided by the Company on ad-hoc basis as and when required (whenever there are changes in the AML Laws, Regulations, Notices, or the Company's AML policy/procedures).

Assessment Criteria

36.8. For Employees who score less than 70% of the total score in the assessment tests followed by the training shall be given a residual training within a period of 30 days and an assessment will be conducted following the same, if the employee fails to pass the residual training for 3 times the matter will be escalated to Senior management for the necessary disciplinary action.

Circulation of AML/CFT Policy

36.9. The CO shall ensure that all the staff are provided with a copy of the AML/CFT Policy and are well educated and trained in compliance with the AML/CFT policy. The CO must provide all the employees with an approved AML policy upon joining for their acknowledgement and obtain an undertaking letter from them declaring that they fully have read and understood the AML Policy and will comply and establish with the same.

37. CUSTOMER EXIT POLICY

37.1. The Company adheres to the following guidelines when exiting a relationship with a Customer:

Termination by Law

- Upon receiving a court order concerning an existing or registered Customer.
- When required to comply with directives from the EOCN, FIU, or equivalent regulatory bodies.
- Following instructions from the UAE Police Department.
- Any other legal obligation as mandated by law.

Sanction List

- If the Customer is listed for Money Laundering or Terrorism Financing activities.

- If the Customer is found to be involved in severe crimes, such as human trafficking, smuggling, narcotics dealing, tax evasion, or corruption.
- If the individual/entity appears on sanctions lists issued by EOCN, MENAFATF, OFAC, UN, or similar organizations.
- When a Customer is identified as a Politically Exposed Person (PEP), termination requires approval from the Board of Directors (BOD).
- Any other issues related to inclusion in sanctions lists.

Other Reasons

- Discovery of fraudulent attempts or activities by the Customer.
- Mutual agreement to terminate the relationship.
- Any violation, unethical conduct, or other circumstances requiring the closure of the client relationship to protect the Company's reputation and ensure regulatory compliance.

37.2. When any of the above situations occur, the Company will terminate the relationship with the Customer and report the incident to the relevant regulatory authorities. Additionally, the Customer's name will be added to an internal blacklist to safeguard the integrity of the Client Exit process.

Re-Onboarding of Exited Customers

37.3. Should the Company decide to re-initiate a relationship with an exited Customer, the following procedures will be implemented:

- Obtain approval from Senior Management for re-onboarding.
- Conduct a full KYC process for the Customer and Ultimate Beneficial Owner (UBO) in compliance with regulations.
- Perform screening of the entity, all shareholders, and authorized representatives against relevant negative lists.

38. RECORD RETENTION

38.1. Our Company recognizes the importance of maintaining comprehensive records related to AML and CFT efforts. The following documents will be considered as our Company's AML/CFT Documents:

- **Clients' Documentation:** This includes all documentation provided by clients as part of the KYC checklist and correspondences. It encompasses documents obtained during CDD and EDD processes. These records are essential for establishing and verifying the identity of clients and assessing potential risks associated with them.
- **Suspicious Activity Reports:** Our Company will maintain records of all suspicious activity reports (SARs) concerning clients or applicants. This includes any response or follow-up actions taken regarding the reported suspicious activities. These records are crucial for tracking and documenting potential illicit activities and the steps taken to address them.

- **AML/CFT Training Records:** Our Company will keep records of AML/CFT training sessions attended by staff, officers, and affiliates. These records will include the dates, content, and attendees of the training sessions. They demonstrate commitment to educating and updating personnel on AML/CFT obligations and best practices.
- **AML/CFT Committee Minutes of Meeting:** Records of minutes of meetings of the AML/CFT Committee will be maintained. These minutes will document the details of all decisions made by the committee, ensuring transparency and accountability in AML/CFT efforts.
- **Senior Management Decisions:** Our Company will retain records of all AML/CFT decisions made by the senior management. These records demonstrate the involvement and commitment of senior management in implementing effective AML/CFT measures.

38.2. The objective of keeping these records is to ensure that our Company can provide basic information for the reconstruction of transactions when requested by competent authorities. The documents may be retained as originals or copies, including scanned images stored in various electronic formats such as pen drives, hard discs, online systems, cloud-based systems, etc., if they are admissible in UAE Court of Law.

38.3. Our Company will designate at least two people responsible for the safekeeping of these records, ensuring their security and confidentiality. Additionally, all records must be easily accessible to relevant authorities when required. Requests for such records by government authorities will be fulfilled within a reasonable time frame, not exceeding fifteen (15) business days.

38.4. By maintaining comprehensive AML/CFT records, our Company aims to demonstrate compliance with regulatory requirements and facilitate effective cooperation with competent authorities in combating money laundering, financing of terrorism and illegal Organisations.

39. RECORD RETENTION POLICY

39.1. Our Company shall adhere to the following document retention periods:

- All records of transactions involving the clients, including customer identification records, must be maintained, and securely stored, either physically or digitally, in an easily accessible location for a period of five (5) years from the date of the transaction.
- In the case of closed accounts, records pertaining to customer identification, account files, and business correspondence must be preserved and securely stored for a minimum of five (5) years from the date of closure.
- If the records are related to an ongoing investigation or transactions that have been the subject of a disclosure, they must be retained beyond the specified retention period until the FIU confirms that the case has been closed.

39.2. By adhering to these document retention periods, our Company ensures compliance with regulatory requirements and facilitates the availability of relevant information for auditing, monitoring, and investigation purposes.

40. ONGOING MONITORING

40.1. The Company shall undertake CDD measures and ongoing supervision of business relationships, including ensuring that the documents, data, or information obtained under CDD Measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories.

40.2. The CO shall conduct a periodic review of customer information, particularly for high-risk customers and transactions, to ensure that documents are valid and relevant.

40.3. Such reviews shall take place at least:

- For Low Risk Profile Clients – once every 3 years;
- For Medium Risk Profile Clients – once every 2 years;
- For High Risk Profile Clients – once every 1 year.

41. INDEPENDENT AUDIT

41.1. The Internal Auditors function as a third line of defence in AML & CFT compliance framework at the Company, first being business functions and second being the Compliance Department. The Company understands that internal audit is an integral part of the governance framework, thus the Company has outsourced the internal audit function to an external party and ensure that periodic assessment of effectiveness of the AML & CFT compliance program and present its findings and report the Owner

41.2. Internal Audit shall ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front-line staff of their responsibilities in this regard.

41.3. A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. Ashkenazi Trading confirms to have in place an independent audit function to test the effectiveness and adequacy of their internal polices controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations. The scope of such audits should include but not be limited to:

- Examine the 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.

42. REPORTING TO FINANCIAL INTELLIGENCE UNIT (FIU)

42.1. The core function of the FIU is to conduct operational analysis on STRs, and information received from FIs, other companies as well as from Competent Authorities, and to support the investigations of Law Enforcement Authorities. It does so by identifying specific targets (such as persons, funds, or criminal networks) and by following the trail of specific transactions in order to determine the linkages between those targets and the possible proceeds of crime, money laundering, predicate offences, and terrorist financing.

43. SUSPICIOUS TRANSACTION REPORT/ SUSPICIOUS ACTIVITY REPORT (STR/SAR)

43.1. Any suspicious transactions or activities that do not include confirmed or potential matches to the UAE Local Terrorist List or UN Consolidated List should be reported to the FIU by raising a STR/SAR through the goAML platform.

43.2. The Company will ensure to file any the Suspicious Transaction Reports / Suspicious Activity Reports on the GoAML portal upon receipt of any iSTR' s received from the FLA's and scrutinization of the said cases by the Compliance Department.

44. DEALERS IN PRECIOUS METALS & STONES REPORT (DPMSR)

44.1. In addition to the due diligence and reporting requirements mentioned in other sections of this policy, our Company, in accordance with Circular Number: 08/AML/2021 issued by the Ministry of Economy, UAE, will be complying with the following due diligence and reporting requirements:

- Transactions with resident individuals: Obtain identification documents (Emirates ID or Passport) for cash transactions equal to or exceeding AED 55,000 and register the information in the FIU's GoAML platform using the DPMSR.
- Transactions with non-resident individuals: Obtain identification documents (ID or Passport) for cash transactions equal to or exceeding AED 55,000 and register the information in the FIU's GoAML platform using the DPMSR.
- Transactions with entities / companies: Obtain a copy of the trade license, and identification documents (Emirates ID or passport) of the person representing the company, in transactions equal to or exceeding AED 55,000 in cash or through wire transfer and register the information in the FIU's GoAML platform using the DPMSR.
- Keep records of all documents and information related to the above transactions for a minimum period of 5 years.

45. EXCEPTIONS: (NOT TO REPORT)

45.1. AED Settlement where both the parties have accounts in the same bank in the UAE.

45.2. AED Settlement where both the parties have accounts in different banks in the UAE.

45.3. USD Settlement where both the parties have accounts in same bank in the UAE.

45.4. Trade between related parties Mainland to Free zone having same bank account transactions and Vice Versa.

45.5. Barter transaction (Exchange of Gold)

45.6. Intra Company Transactions

45.7. Transaction is not routed through the UAE Bank Account.

46. HIGH RISK JURISDICTION TRANSACTIONS REPORTING

46.1. Business relationships or transactions involving natural person or legal entities from high-risk jurisdictions must be reported to Financial Intelligence Unit (FIU) by CO (through the Go AML Portal).

46.2. Such reported transactions may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.

46.3. The obligation for reporting as well as putting it on hold is for cross-border transactions through banking or remittance channels. It includes transactions which originate from, are destined to, or are routed through the High-Risk Jurisdictions.

46.4. The transactions also include cross border transactions from/to any country where the remitter or the beneficiary is individual or legal entity associated with high-risk jurisdictions. Individuals are associated with High-Risk Jurisdictions by virtue of Nationality or Residence. Legal Entities are associated with High-Risk Jurisdiction by virtue of its Place of Incorporation or if it is controlled by or its authorized signatory is an Individual from the High-Risk Jurisdiction.

47. FUND FREEZE REPORTS

47.1. In case a confirmed match is identified, the reporting entity must freeze without delay all funds and submit an FRR 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.

47.2. The Company will ensure to file any Fund Freeze Reports, if necessary, in the GoAML portal upon receipt and scrutinization of any confirmed match by the Compliance Department.

48. PARTIAL NAME MATCH REPORT (PNMR)

48.1. In case a potential/partial name match is identified, the reporting entity 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, along with all the necessary information and documents

regarding the name match are submitted and maintain suspension measures related to the potential match until further instructions are received from Executive Office via goAML on whether to cancel the suspension ('false positive') or implement freezing measures ('confirmed match').

48.2. The Company will ensure to file any Partial Name Match Reports, if necessary, in the GoAML portal upon receipt and scrutinization of any partial name match by the Compliance Department.

49. INFORMATION REQUEST FROM FIU (RFI)

49.1. As part of its obligations to comply with anti-money laundering and counter-terrorism financing regulations, the Company may receive information requests from the FIU (Financial Intelligence Unit). In such cases, the Company must ensure that it responds to these requests in a timely and accurate manner.

50. TIPPING OFF AND CONFIDENTIALITY

50.1. Tipping off a customer refers to the unauthorized act of disclosing information that could lead the customer or a third party to become aware or suspect that they are the subject of a suspicious transaction report, or an investigation related to money laundering or terrorist financing.

50.2. It also includes disclosing information that could prejudice the prevention or detection of offenses, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorist financing.

50.3. Our Company directors, officers, and employees are strictly prohibited from warning customers about the reporting of information to the FIU or communicating such information to anyone other than the FIU. Any violation of this confidentiality provision can result in criminal, civil, and administrative sanctions under the UAE AML/CFT law.

50.4. It is essential for our Company to maintain the confidentiality of information related to suspicious transactions and investigations to ensure the effectiveness of AML or CFT efforts.

51. BI – ANNUAL COMPLIANCE REPORTS

51.1. The CO shall prepare and present bi-annual report on AML/CFT Compliance Function in order to assess the effectiveness of the AML/CFT policies, procedures, systems, and controls to prevent ML/TF.

51.2. The Bi-Annual Compliance Reports must be submitted within one (1) month from the end of each reporting period to the Owner for his review and approval.

51.3. Such a report shall include, but not limited to: -

- Assessment of ML/FT risks associated with the business and the effectiveness of its policies, procedures, systems, and controls.
- Summary of the gap analysis between the AML/CFT Program and existing AML Laws, Regulations, Notices, and the Guidelines as well as the actions taken by the CO to bridge or resolve such gaps.

- The number of internal suspicious disclosures made by employees and the number of cases investigated, closed, kept open for future monitoring, or reported to the FIU as STRs during the reporting period.
- The number of suspicious transactions detected and reported to the FIU via independent transaction monitoring by the CO during the reporting period.
- Changes in the AML/CFT policies and procedures reviewed and the details of any AML/CFT policy or procedures newly introduced during the reporting period.
- Statistics on the total employees, new joiners during the reporting period, number of employees trained, and the number of employees not trained (if any) including reasons for not training employees.
- Recommendations to the Owner for the improvement of the AML/CFT function.
- Details of CO's requests for additional human resources, systems, controls, tools, and technology changes for the attention of the Owner.
- The conclusion of the CO about the effectiveness of the existing AML/CFT function.

52. NO RETALIATION POLICY

52.1. The Company is committed to maintaining a culture of compliance with all applicable anti-money laundering (AML) and countering the financing of terrorism (CFT) laws, regulations, and policies. As part of this commitment, the Company strictly prohibits any form of retaliation against employees who report any concerns or suspected violations of AML/CFT regulations, policies, or procedures.

52.2. The Company values and encourages the reporting of any such concerns, and will not tolerate any form of retaliation, including but not limited to, termination, demotion, denial of promotion or training, or any adverse employment action against employees who report any AML/CFT concerns in good faith. As a result of their good faith performance of their statutory obligations to comply with this Policy, all 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.

52.3. Any employee who believes that they have been retaliated against for reporting any AML/CFT concerns is encouraged to report the matter immediately to their supervisor, or to the CO. The Company will investigate all such reports promptly, thoroughly, and confidentially, and will take appropriate remedial action, up to and including disciplinary action, against any employee found to have retaliated against another employee for reporting any AML/CFT concerns.

53. REVIEW

53.1. The Company conducts a periodic review of the policy. In case of amendment in statutory provisions/ regulations necessitating amendment, the relevant portions of policy shall be deemed to have been modified from the date of amendment in relevant statutory provisions. In such cases, the modified policy shall be placed for review by the Board in a regular course.

53.2. A regular review of the "Compliance Manual" shall be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources and should be accompanied by a formal assessment or written report. If and when regulations are amended concerning reporting of suspicious activities, Ashkenazi Trading will amend the Compliance Manual to comply with those regulations.

Scope:

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

54. COMMUNICATION

54.1. The Compliance Officer shall ensure that this policy is communicated to all management and relevant staff including Customers and all concerned.

55. DISCLAIMER

55.1. The following provisions are included in the policy to ensure compliance and accountability:

1. **Reporting Obligations:** Employees must immediately report to management if they suspect or have reason to believe that Ashkenazi Trading may have been or is being exposed to funds from a suspicious or doubtful source.
2. **Policy Violations:** Employees who violate the terms of this Policy will face disciplinary actions, which may include termination of employment.

3. **Failure to Report:** Employees with direct knowledge of potential or apparent violations of this Policy who fail to report such acts to Company management will be subject to disciplinary measures.
4. **Obstruction of Investigations:** Employees who knowingly mislead or obstruct investigations into reported violations of this Policy or applicable laws will be held accountable and may face disciplinary actions.
5. **Disciplinary Actions for Third Parties:** Third parties associated with Ashkenazi Trading 's operations who violate the terms of this Policy risk having their contracts reviewed, re-evaluated, or terminated.

55.2. These measures are implemented to uphold the integrity of Ashkenazi Trading 's operations and ensure compliance with applicable laws and regulations.

****

ANNEXURE – 1 GLOSSARY

AML	Anti-Money Laundering
CBUAE	Central Bank Of UAE
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
CO	Compliance Officer
CP	Customer Profile
DNFBPs	Designated Non-Financial Business and Professions
DPMS	Dealers in Precious Metal and Stones
EDD	Enhanced Due Diligence
EOCN	Executive Office for Control and Non-Proliferation
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FPEP	Foreign Politically Exposed Person
KYC	Know Your Customer
CO	Money Laundering Reporting Officer
MENAFATF	Middle East and North Africa FATF
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PF	Proliferation of Funds
PMS	Precious Metal and Stones
RBA	Risk Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TF	Terrorist Financing
UBO	Ultimate Beneficial Owners
UN	United Nations
WMD	Weapons and Mass Destruction

ANNEXURE – 2 DEFINITIONS

AML / CFT	Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Beneficial owner	The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client; 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.
Client /Customer	Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law with one of the financial institutions or designated nonfinancial businesses and professions.
Competent Authorities	The competent government authorities in the State entrusted with the implementation of any provision of this Decree Law
Confiscation	Permanent expropriation of private funds or proceeds or instrumentalities by an injunction issued by a competent court.
Controlled Delivery	The process by which a competent authority allows the entering or transferring of illegal or suspicious funds or crime revenues to and from the UAE for the purpose of investigating a crime or identifying the identity of its perpetrators.
Crime	Money laundering crime and related predicate offences, or financing of terrorism or illegal organizations.
Customer Due Diligence (CDD)	The process of identifying or verifying the information of a client 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 purpose of this Decree-Law and its Implementing Regulation.
Decree- Law	Federal Decretal-Law No. (20) of 2018 on Anti- Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.

Designated Non-financial Businesses & Professions	Anyone who conducts one or several of the commercial or professional activities defined in the Cabinet Decision No.10 of 2019.
CAHRA	Conflict-Affected and High-Risk Areas
Financial institutions	Anyone who conducts one or several of the activities or operations defined in the Implementing Regulation of the present Decree Law for the account of /or on behalf of a client.
Financing Illegal Organizations	Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or its members.
Financing of Terrorism	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014
Freezing or seizure	Temporary attachment over the moving, conversion, transfer, replacement or disposition of funds in any form, by an order issued by a competent authority.
Funds	Assets in whatever form, tangible, or intangible, movable or immovable including national currency, foreign currencies, documents, or notes evidencing the ownership of those assets or Associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.
High Risk Customer	A Customer who represents a risk either in person, activity, business relationship, nature of geographical area, such as a Customer from a high-risk country or non-resident in a country in which he does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by financial institutions, or designated non-financial businesses and professions, or the Supervisory Authority.
Illegal Organizations	Organizations whose establishment is criminalized, or which exercise a criminalized activity

Law-enforcement Authorities	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidence on the crimes including AML/CFT crimes and financing illegal organizations
Legal Arrangement	A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as trust funds or other similar arrangements.
Legal person	Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.
Local Terrorist List	Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) Paragraph (I) of Federal Law No. (7) of 2014 on Combating Terrorism Offences.
Means	Any means used or intended to be used to commit an offence or felony.
Money Laundering	Any of the acts mentioned in Clause (1) of Article (2) of the present Decree-Law
Non-Profit Organizations	Any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit legal arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities.
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 organizations or any prominent function within such an organizations; 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 favor of the PEP.
Predicate Offence	Any act constituting an offense or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries
Proceeds	Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
Purpose of transaction	An explanation about why a customer is conducting a transaction or the reason for which the funds will be used. Examples of purpose of transaction are - family support, education, medical, tourism, debt settlement, financial investment, direct investment, or trading etc. For verification of the purpose of transaction, documents may include any documentation proving the purpose for which the money will be used.
Registrar	The entity in charge of supervising the register of commercial names for all types of establishments registered in the UAE.
Settlor	A natural or legal person who transfers the control of his funds to a Trustee under a document.
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.
Source of funds	Means the origin of customer's funds which relate to a transaction or service and includes how such funds are connected to a customer's source of wealth.
Source of wealth	Means how the customer's global wealth or net worth is or was acquired or accumulated
Supervisory Authority	Federal and local authorities which are entrusted by legislation to supervise financial institutions, designated non-financial businesses and professions and non-profit organizations or the competent authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations

Suspicious Transactions	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanor or felony or related to the financing of terrorism or of illegal organizations, whether committed or attempted.
Targeted Financial Sanctions (TFS)	The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings, The term Targeted Financial Sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups or organizations who are sanctioned.
The Executive Office	The Executive Office of the Committee for Goods and Materials Subject to Import and Export control.
Transaction	All disposal or use of Funds or proceeds including for example deposits, withdrawals, conversion, sales, purchases, Inward remittance, outward remittance.
Ultimate Beneficial Owner	A person (natural) who owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a juridical person. A Natural Person who owns 25% or above of the juridical person is treated as a UBO.
UN Consolidated List	A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.
Undercover Operation	The process of search and investigation conducted by one of the judicial impoundment officer by impersonating or playing a disguised or false role to obtain evidence or information related to the Crime.
Wire Transfer	Financial transaction conducted by a financial institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether the transferor and the beneficiary are the same person.
Without Delay	Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

ANNEXURE – 3 HIGH-RISK / MONITORED JURISDICTIONS

High-Risk Jurisdiction under increased Monitoring (updated as of February 2025)

Countries	Status
Algeria	Grey List
Angola	Grey List
Bulgaria	Grey List
Burkina Faso	Grey List
Cameroon	Grey List
Côte d'Ivoire	Grey List
Croatia	Grey List
Democratic Republic of Congo	Grey List
Haiti	Grey List
Kenya	Grey List
Lao People's Democratic Republic	Grey List
Lebanon	Grey List
Mali	Grey List
Monaco	Grey List
Mozambique	Grey List
Namibia	Grey List
Nepal	Grey List
Nigeria	Grey List
South Africa	Grey List
South Sudan	Grey List
Syria	Grey List
Tanzania	Grey List
Venezuela	Grey List
Vietnam	Grey List
Yemen	Grey List

High-Risk Jurisdiction subject to Call for Action (updated as of February 2025)

Countries	Status
Iran	High-Risk Jurisdiction
Democratic People's Republic of Korea (DPRK)	High-Risk Jurisdiction
Myanmar	High-Risk Jurisdiction

ANNEXURE – 4 LIST OF CAHRAS

Region	Country	Risk Factors	Sanctions / Watchlists
Africa	Sudan	Armed conflict, terrorism, human rights violations	UN, EU, US Sanctions
	South Sudan	Ongoing civil war, corruption, human rights issues	UN, US Sanctions
	Democratic Republic of Congo	Conflict minerals, corruption, militia violence	US Dodd-Frank Act, UN
	Central African Republic	Political instability, war crimes	UN, EU Sanctions
	Somalia	Terrorism (Al-Shabaab), weak governance	UN, US Sanctions
	Libya	Civil war, terrorism, human trafficking	UN, US, EU Sanctions
	Mali	Terrorism, insurgencies, illicit trade	UN, EU Sanctions
	Burkina Faso	Islamist insurgency, violence against civilians	UN, EU Sanctions
Middle East	Syria	Civil war, terrorism, chemical weapons	UN, US, EU Sanctions
	Yemen	Ongoing war, humanitarian crisis, arms smuggling	UN, US, EU Sanctions
	Iraq	Post-war instability, terrorism	UN, US, EU Sanctions
	Iran	Terrorism financing, nuclear proliferation	UN, US, EU Sanctions
Asia	Afghanistan	Taliban control, terrorism, opium trade	UN, US Sanctions
	Myanmar	Ethnic conflict, military junta	UN, US, EU Sanctions
Europe	Ukraine (Eastern regions)	Russia-Ukraine conflict, war crimes	UN, US, EU Sanctions
Americas	Venezuela	Political instability, corruption	US, EU Sanctions

For detailed list, visit https://www.cahraslist.net/cahras

ANNEXURE – 5 HIGH-RISK FACTORS

1. Customer Risk Factors

- The business relationship is conducted in unusual circumstances.
- Non-resident customers.
- Legal persons or arrangements that are personal asset-management vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Businesses or activities that are cash-intensive or particularly susceptible to money laundering or terrorism financing.
- The ownership structure of the Company appears unusual or excessively complex given the nature of the Company's business.
- Business relationships and transactions conducted other than "face to face".
- Business relationships conducted in or with countries as identified in (b) below.
- Politically exposed persons ("PEP").
- High net worth customers, or customers whose source of income or assets is unclear.

2. Country or Geographic Risk Factors

- Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
- Countries identified by the Committee as high risk.
- Countries subject to sanctions, embargos or similar measures issued by the United Nations.
- Countries classified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

3. Product, Service, Transaction, or Delivery Channel Risk Factors

- Cash and other bearers or negotiable instruments.
- Accounts open, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
- Payment received from unknown or unassociated third parties.