

# **POLICY MANUAL**

## **ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND FINANCING OF ILLEGAL ORGANIZATIONS**

**ASHKENAZI TRADING DMCC**

**AML/CFT Policy Manual  
Version Control (V. 1.0)  
2023**



## CONTENTS

Glossary .....	4
1. Introduction.....	5
2. Purpose & Rationale.....	6
3. Definition of Money Laundering, Financing of Terrorism, and Illegal Organization.....	8
4. Legal and Regulatory Framework.....	11
5. Ashkenazi Trading Services.....	15
6. Policy Scope .....	16
7. Governance of Risk .....	16
8. Policy Governance .....	17
9. Commitment Statement.....	19
10. Risk Factors relating to Ashkenazi Trading .....	20
11. ML/TF Risks to be considered by Ashkenazi Trading .....	23
12. Cash Policy.....	24
13. Role of the Key Members .....	24
14. Compliance Function .....	26
15. Policy Custodian .....	28
16. Periodical Review .....	29
17. Compliance Internal Audit.....	30
18. Procedure and Controls (General).....	31
19. Identification, Verification, and Know Your Customer .....	32
20. Risk-Based Approach.....	34
21. KYC Process .....	35
22. Customer Onboarding.....	36
23. Customer Due Diligence.....	39
24. Enhanced Due Diligence.....	40
25. Politically Exposed Persons .....	42
26. Sanctioned Individuals/Entities.....	43



27. Updating KYC Information..... 44

28. Monitoring of Client's Activities..... 44

29. Indicators of Suspicious Activities - Red Flags ..... 45

30. Targeted Financial Sanctions (TFS) ..... 50

31. TFS Obligations.....51

32. Ongoing Screening..... 55

33. Reporting of Suspicious Activities/Transactions..... 56

34. Dealers in Precious Metals and Stones Report (DPMSR) .....57

35. Process of Submitting TFS Report .....57

36. Tipping Off and Confidentiality ..... 60

37. Training and Awareness..... 60

38. Record Keeping .....61

39. Record Retention Policy.....62

40. Revision Record .....63

APPENDIX A – KYC Documents Checklist – Individual ..... 64

APPENDIX B – KYC Documents Checklist – Corporate..... 66



## Glossary

*AML* Anti-Money Laundering

<i>AML</i>	Anti-Money Laundering
<i>AML</i>	Anti-Money Laundering and Combating the Financing of Terrorism Supervision Department
<i>CDD</i>	Customer Due Diligence
<i>CFT</i>	Combating the Financing of Terrorism
<i>CBUAE</i>	Central Bank of the UAE
<i>DMCC</i>	Dubai Multi Commodities Centre Authority
<i>EDD</i>	Enhanced Due Diligence
<i>EOCN</i>	Executive Office for Control & Non-Proliferation
<i>EU</i>	European Union
<i>Executive Office – IEC</i>	Executive Office of the Committee for Goods and Materials Subject to Import and Export Control
<i>FATF</i>	Financial Action Task Force
<i>FIU</i>	Financial Intelligence Unit
<i>FT</i>	Financing Terrorism
<i>ID</i>	Identification
<i>INTERPOL</i>	International Police Organization
<i>KYC</i>	Know Your Customer
<i>ML</i>	Money Laundering
<i>MLRO</i>	Money Laundering Reporting Officer
<i>MOE</i>	Ministry of Economy
<i>OECD</i>	Organisation for Economic Co-operation and Development
<i>OFAC</i>	Office of Foreign Assets Control
<i>PEP</i>	Politically Exposed Person
<i>PMS</i>	Precious Metals and Stones
<i>SAR</i>	Suspicious Activity Report
<i>STR</i>	Suspicious Transaction Report
<i>TFS</i>	Targeted Financial Sanctions
<i>UAE</i>	United Arab Emirates
<i>UBO</i>	Ultimate Beneficial Owner
<i>UN</i>	United Nations



## 1. Introduction

- 1.1. In the current era, where financial crimes and illicit activities have become increasingly sophisticated, it is crucial for organizations to adopt robust measures to combat money laundering. Ashkenazi Trading DMCC (hereinafter referred as '**Ashkenazi Trading**'), based in the United Arab Emirates (UAE), recognizes the significance of this issue, and has developed a comprehensive compliance policy and procedure manual to address anti-money laundering (AML) and combating the financing of terrorism and illegal organizations.
- 1.2. The compliance policy serves as a guiding framework, reflecting our organization'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.
- 1.3. 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.
- 1.4. Through the implementation of this compliance policy, we aim to foster a culture of compliance within our organization. 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.
- 1.5. 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.
- 1.6. By implementing and adhering to this compliance policy, Ashkenazi Trading aims to contribute to global efforts in combating money laundering, the financing of terrorism, and the financing of illegal organizations, thereby safeguarding the integrity of the financial system. We strongly believe that by taking these measures, Ashkenazi Trading can foster a



more transparent and secure business environment, while minimizing the risk of financial crimes.

- 1.7. 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 Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Financing of Illegal Organizations. All personnel at Ashkenazi Trading 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 within Ashkenazi Trading. 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 Ashkenazi Trading fully complies with the relevant national legislation pertaining to AML, CFT, and financing of illegal organizations. 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 Ashkenazi Trading remains vigilant in identifying and addressing potential risks.
  - **Enhance Risk Management:** Implementing a compliance policy enhances the Ashkenazi Trading' overall risk management framework by identifying and addressing money laundering and terrorist financing risks. The policy enables Ashkenazi Trading 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, Ashkenazi Trading safeguards its reputation and maintains the trust of its



stakeholders. The policy demonstrates the company'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, Ashkenazi Trading 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 the financing of terrorism (CFT). Terrorist organizations 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 Ashkenazi Trading 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 the entire organization remains vigilant in preventing money laundering.

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

- **Legitimate Source of Funds:** Ashkenazi Trading 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, Ashkenazi Trading aims to prevent money laundering activities and avoid unwittingly facilitating illicit financial transactions.
- **Risk to Reputation and AML/CFT Commitment:** Ashkenazi Trading 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 Ashkenazi Trading' reputation or compromise its commitment to AML/CFT standards.



### 3. Definition of Money Laundering, Financing of Terrorism, and Illegal Organization

- 3.1. 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. Organizations 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.
- 3.2. 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 anti-money laundering and counter-terrorism financing efforts. The country has also actively engaged in international collaborations and partnerships to enhance its capabilities in this area.
- 3.3. 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

- 3.4. 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.
- 3.5. 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.



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

3.7. 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.

3.8. 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

3.9. 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.

3.10. 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 organization 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 organization or individual involved in terrorism, while being aware of the true background or purpose behind these actions.

### Financing of Illegal Organizations

3.11. The AML/CFT Law defines Financing of Illegal Organizations as:

- Engaging in any form of money laundering, while being aware that the proceeds, whether wholly or partially, are owned by an illegal organization or any individual associated with an illegal organization 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 organization or any of its members, while being aware of the identity or purpose of the organization.

#### 4. Legal and Regulatory Framework

##### National Legislative and Regulatory Framework

- 4.1. 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.
- 4.2. 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 Organizations (NAMLCFTC) was established in 2000. Its primary role is to oversee and coordinate anti-money laundering (AML) policies and initiatives in the UAE. The committee's focus is on enhancing the effectiveness of the AML and combating the financing of terrorism (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.
- 4.3. 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 (AMLSD). This department is responsible for handling all matters related to anti-money laundering and combating the financing of terrorism (AML/CFT) within the UAE. The AMLSD works closely with the UAE's National AML/CFT Committee to effectively implement the National Action Plan.
- 4.4. 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.



4.5. 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

- Federal Decree-Law No. (20) Of 2018 On 'Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations'.
- Federal Decree Law No (26) of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
- 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

- 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 Organizations'.
- Cabinet Resolution No (24) of 2022 amending some provisions of Cabinet Resolution No (10) of 2019 On the Executive Regulations of Federal Decree-Law No (20) of 2018 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations
- Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures.
- Cabinet Resolution No. (53) of 2021 Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Resolution No. (58) of 2020 Concerning the Regulation of Beneficial Owner Procedures.
- 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 Decision

- 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 the international judicial cooperation in the distribution of the proceeds of crime.

#### Circular

- Circular No. 02 of 2021 issued by Ministry of Economy United Arab Emirates.
- Circular No. 09 of 2021 regarding GoAML reporting requirements.
- 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 update 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.

#### Miscellaneous

- 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 organizations.



- Guidelines for Financial Institutions on Anti-Money laundering and combating the financing of terrorism and illegal organizations issued by the UAE Central Bank on 23.06.2019.

*International Legislative and Regulatory Framework*

- 4.6. 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 organizations that serve as global standard setters in this domain. These organizations 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.
- 4.7. The AML/CFT legislative and regulatory framework in the UAE is an integral part of a broader international framework that addresses anti-money laundering and combating the financing of terrorism. This international framework consists of intergovernmental legislative bodies and international and regional regulatory organizations.
- 4.8. 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 member countries then incorporate these international laws into their respective national legal frameworks.
- 4.9. In tandem with intergovernmental legislative bodies, international and regional regulatory organizations play a crucial role in developing policies and recommending, assessing, and monitoring the implementation of international regulatory standards related to AML/CFT. These organizations work to ensure consistent adherence to best practices and standards across participating member countries.
- 4.10. Together, these intergovernmental legislative bodies and international/regional regulatory organizations collaborate to establish a comprehensive and harmonized global approach to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction.
- 4.11. 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 organizations. Some of these organizations 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 organization that aims to enhance AML/CFT efforts and cooperation among its member countries in the Middle East and North Africa region.

4.12. These are just a few examples of the intergovernmental and international/regional organizations 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.

## 5. Ashkenazi Trading Services

- 5.1. 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.
- 5.2. 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.
- 5.3. In line with its dedication to regulatory compliance, Ashkenazi Trading Services has successfully registered on the GoAML portal. This registration demonstrates the company's



proactive approach to combatting money laundering and terrorist financing. Additionally, Ashkenazi Trading has completed the registration process with the website of the Executive Office of Control and Non-Proliferation (EOCN). This registration allows Ashkenazi Trading to receive important notifications regarding inclusion and removal from terrorist lists, reaffirming its unwavering commitment to upholding regulatory compliance standards.

## 6. Policy Scope

- 6.1. 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 Ashkenazi Trading.
- 6.2. It is the responsibility of Ashkenazi Trading 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 Ashkenazi Trading reserves the right to take appropriate action, including additional measures, as deemed necessary to ensure the diligent implementation and enforcement of this Policy.
- 6.3. If Ashkenazi Trading, 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.
- 6.4. If a client of Ashkenazi Trading breaches any provisions of this Policy, Ashkenazi Trading 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.
- 6.5. By implementing these measures, Ashkenazi Trading aims to maintain a high level of compliance with anti-money laundering and counter-terrorism financing standards and ensure the integrity and reputation of the organization while fulfilling its obligations to prevent and detect any illicit activities.

## 7. Governance of Risk

- 7.1. To effectively manage and mitigate the risks associated with anti-money laundering and countering the financing of terrorism (AML/CFT), Ashkenazi Trading 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.

- 7.2. Operations - This represents the first line of defense. As the frontline function for Know Your Customer (KYC) and Customer Due Diligence (CDD), Ashkenazi Trading 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.
- 7.3. 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. Ashkenazi Trading will also establish criteria for categorizing clients based on risk levels and monitor any suspicious transactions.
- 7.4. Internal Audit - This constitutes the third line of defense. This independent function provides assurance by assessing whether appropriate controls have been established. Ashkenazi Trading 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.
- 7.5. By implementing these three lines of defense, Ashkenazi Trading aims to establish robust AML/CFT measures to identify and mitigate risks associated with money laundering and terrorist financing.
8. Policy Governance
  - 8.1. Ashkenazi Trading has established an AML/CFT Committee to oversee and implement the AML/CFT procedures within the company. The committee has a broad mandate, including the responsibility of monitoring and coordinating the identification, assessment, and response to the risks associated with money laundering and terrorism financing. This ensures that Ashkenazi Trading maintains a strong and appropriate AML/CFT structure.
  - 8.2. The AML/CFT Committee will hold a minimum of four regularly scheduled meetings per year to discuss AML/CFT matters, review action plans, and recommend follow-up actions



based on the outcomes of the reviews. Ideally, the committee aims to hold at least one meeting per quarter, ensuring that the gap between two committee meetings does not exceed six months. During these meetings, the committee will discuss initiatives to continually improve Ashkenazi Trading achievements in the AML/CFT area.

8.3. The AML/CFT Committee will maintain written minutes or records of its meetings and activities. The minutes of each meeting will be distributed to every member of the committee, ensuring transparency and accountability.

8.4. The structure of the AML/CFT Committee will consist of the following members:

- Head of the Committee: General Manager
- Members: Compliance Officer, Head of Operations, Head of Accounts, Accounts Executive, Head of Sales

8.5. The key responsibilities of the AML/CFT Committee will include:

- Preparing a policy and process manual for implementing the provisions of UAE's Federal Decree-Law No. (20) Of 2018 and Cabinet Decision No. (10) Of 2019.
- Ensuring the proper implementation and effectiveness of procedures and processes to combat money laundering and terrorism financing within Ashkenazi Trading.
- Developing a staff training program on methods of controlling financial and banking operations in accordance with the control procedure guide and other relevant legal and regulatory texts.
- Periodically reviewing and updating procedures and processes in line with the latest methods and guidance on combating money laundering and terrorism financing.
- Assessing the company's approach to risk identification, assessment, and mitigation plans for legal and regulatory compliance risks and reviewing the results.
- Establishing an effective customer identification and due diligence program for onboarding and maintaining customer relationships.
- Reviewing resources, systems, and tools available to the Compliance Officer and ensuring they are up to date with international and national standards and appropriate for the company's nature, size, and complexity.
- Reviewing internal audit findings and making suggestions for necessary modifications to the Compliance Program.
- Addressing ongoing challenges/issues in the implementation of AML/CFT procedures and processes and ensuring appropriate controls are in place to mitigate or resolve them.
- Taking corrective/preventive actions when gaps or deficiencies are identified.



- Discussing current and emerging legal and regulatory compliance risks and enforcement trends that may impact the company's business operations, performance, or strategy.
- Reviewing reports submitted by the Compliance Unit regarding adopted procedures, unusual operations, and high-risk customers.
- Defining procedures and processes to be followed by the senior management team when approving business relationships with high-risk customers or executing high-risk transactions.
- Discussing the development of internal programs aimed at promoting an ethical culture within the organization.
- Regularly reviewing significant risk exposures or compliance violations and monitoring the steps taken to address and mitigate them.
- Discussing and making decisions on various areas, including updates on sanctions, notices/circulars from regulatory authorities, suspicious activity reports (SARs) raised during the quarter, enhanced customer due diligence conducted, training conducted and attendance records, feedback/queries from regulatory authorities, pattern analysis conducted, and any newly identified AML/CFT risks.

## 9. Commitment Statement

- 9.1. Ashkenazi Trading, as a responsible organization registered with the Dubai Economic Development, is committed to actively support the domestic and international efforts in combating money laundering, terrorism financing, and the financing of illegal organizations. Ashkenazi Trading recognizes that corporate integrity, which entails upholding strict standards of ethical conduct, is essential for creating sustainable value and maintaining stakeholders' confidence.
- 9.2. The management team at Ashkenazi Trading assumes direct responsibility for compliance with regulatory standards and actively assists in the fight against money laundering and terrorist financing. Ashkenazi Trading emphasizes its dedication to strict compliance with all relevant laws, regulations, and globally recognized best practices in the field of anti-money laundering and counter-terrorism financing. This commitment is reinforced through the publication, implementation, and operation of the policies, processes, and controls outlined in the AML/CFT Policy Document.
- 9.3. Ashkenazi Trading is willing to collaborate and cooperate with government agencies, recognized law enforcement agencies (both domestic and international), and global regulatory bodies such as FATF (Financial Action Task Force), OFAC (Office of Foreign Assets Control), UN (United Nations), EU (European Union), as well as local regulatory authorities like the Central Bank of the UAE (CBUAE) and the Anti-Money Laundering and Combating



the Financing of Terrorism Supervision Department (AMLFD). Ashkenazi Trading aims to actively contribute to joint efforts in combating money laundering and terrorism financing.

- 9.4. To safeguard the interests of all stakeholders, including customers, shareholders, employees, business partners, and the jurisdiction in which the company operates, Ashkenazi Trading maintains the highest operating standards. This entails staying updated on international and national AML/CFT policies, providing ongoing training for staff members, utilizing up-to-date technology and systems that support anti-money laundering and counter-terrorism financing efforts, and actively combating other related financial crimes.
- 9.5. By adhering to these principles and actively participating in collaborative endeavors, Ashkenazi Trading strives to ensure a safe and transparent business environment and fulfill its responsibility in combating money laundering and terrorist financing effectively.

## 10. Risk Factors relating to Ashkenazi Trading

- 10.1. 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 of terrorism, arms trafficking, and sanctions evasion.
- 10.2. 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.
- 10.3. 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 takes place outside the formal financial system.

10.4. 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 complicity.

10.5. Complicit DPMS may knowingly partake in illicit activities and may in turn use their business relationships with Ashkenazi Trading 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 Ashkenazi Trading to deal in the proceeds of crime.

#### Features of DPMS that Increase Risk

10.6. 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, or does not apply appropriate anti-money laundering/combating the financing of terrorism (AML/CFT) controls.

#### Regulatory Environment

10.7. 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 nominally.

10.8. 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.

10.9. 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

10.10. 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, that 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

10.11. 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

10.12. 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 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



## II. ML/TF Risks to be considered by Ashkenazi Trading

II.1. When required to apply AML/CFT measures, Ashkenazi Trading should carefully consider factors such as customer risk, geographic risk, channel risk, and 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 organizations).
- Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter) 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.

## 12. Cash Policy

- 12.1. Currently, Ashkenazi Trading accepts and conducts a portion of its business through cash transactions.
- 12.2. Ashkenazi Trading 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, Ashkenazi Trading actively reports cash transactions. Additionally, Ashkenazi Trading has implemented strict procedures to accurately document cash receipts and report specified transactions.
- 12.3. Ashkenazi Trading 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.
- 12.4. Ashkenazi Trading 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.

## 13. Role of the Key Members

- 13.1. The responsibilities within Ashkenazi Trading for proper supervision, reporting, and compliance with AML/CFT are as follows:

### **Head of the AML/CFT Committee:**

- Responsible for overseeing all activities within Ashkenazi Trading.
- Establishing transparency, honesty, and integrity throughout business operations.
- Implementing a robust compliance program across all products, services, suppliers, customers, and countries in which Ashkenazi Trading operates.
- Ensuring adequate screening procedures are in place when appointing or employing officers or employees.
- Approving the overall business risk assessment for Ashkenazi Trading.
- Reviewing quarterly compliance reports, focusing on high-risk areas.
- Ensuring all employees receive AML/CFT training.



- Approving and implementing the Compliance Policy of the organization.
- Addressing issues raised by the Compliance Officer and Internal Auditor in a timely manner.
- Developing a good knowledge of applicable laws, rules, regulations, notices, and standards related to the DPMS industry in the UAE.
- Establishing the Internal Audit function and reviewing its effectiveness.
- Setting a zero-tolerance tone against fraud.

**Compliance Officer (Authorized Money Laundering Reporting Officer - MLRO):**

- Creating, implementing, and updating the AML/CFT compliance program for Ashkenazi Trading, ensuring compliance with relevant laws, regulations, notices, standards, and international laws.
- Establishing and maintaining AML/CFT policies, procedures, processes, and controls.
- Ensuring compliance by Ashkenazi Trading staff with AML/CFT guidelines and policies.
- Disseminating circulars, resolutions, instructions, and policies issued by UAE Regulatory Agencies related to AML/CFT.
- Acting as a liaison between Ashkenazi Trading and UAE Regulatory Agencies on compliance matters.
- Preparing and submitting written reports on Ashkenazi Trading compliance with AML/CFT guidelines and regulations.
- Conducting gap analysis to assess compliance with existing AML/CFT procedures and laws.
- Designing compliance training programs and providing regular training to employees.
- Receiving and investigating internal suspicious transaction alerts and reporting suspicious cases to the FIU.
- Reporting and filing Suspicious Transaction Reports (STRs) to the FIU when necessary.
- Assisting the FIU with requested information.
- Performing enhanced due diligence for high-risk customers and proactive monitoring for suspicious activities.
- Reviewing and conducting quarterly audits of AML/CFT processes and procedures, reporting findings and gaps to senior management.
- Conducting internal risk assessments and providing mitigation options.



### **Head of Compliance:**

- Implementing Ashkenazi Trading AML/CFT policies and procedures.
- Fulfilling the compliance officer functions of the organization.
- Handling customer onboarding and KYC documentation.
- Conducting Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).
- Liaising with other companies to obtain necessary documents and information.
- Monitoring day-to-day transactions for any unusual, structured, suspicious, and blacklisted activities.
- Monitoring trade-based money laundering and tracing structured transactions.
- Periodically monitoring suspicious accounts.
- Providing guidance to the Compliance Team on identifying suspicious activities and structured transactions.
- Assisting other departments in applying ML rules and regulations to their functions.
- Providing training to the entire staff.
- Reviewing and addressing watchlists and alerts, updating blacklists regularly.
- Collaborating with compliance departments of other companies.
- Establishing internal controls and ensuring adherence to them.
- Maintaining required records as per Ashkenazi Trading AML/CFT policy and procedures.
- Acting as a liaison between the Compliance Officer and Ashkenazi Trading on compliance matters.
- Taking appropriate remedial actions and informing the Compliance Officer of any identified violations.
- Reporting unusual or suspicious transactions to the Compliance Officer.
- Educating staff on AML and CTF procedures and KYC guidelines.

13.2. These roles and responsibilities demonstrate Ashkenazi Trading' commitment to upholding strict AML/CFT standards and ensuring compliance throughout the organization.

## **14. Compliance Function**

14.1. The Compliance function within Ashkenazi Trading plays a crucial role in ensuring adherence to regulatory requirements, including AML/CFT regulations. The Compliance Officer, along with the Compliance Team, is responsible for implementing and maintaining the company's compliance program.



14.2. The compliance team plays a crucial role in preventing and detecting violations related to money laundering, terrorist financing, and other financial crimes. Here are the key responsibilities of the compliance function:

- **Implementing AML/CFT Policies:** The compliance team is responsible for creating, implementing, and updating AML/CFT policies and procedures within Ashkenazi Trading. These policies should be aligned with local and international laws and regulations.
- **Monitoring Compliance:** The compliance team monitors the day-to-day operations of the organization to ensure compliance with AML/CFT guidelines. They conduct regular reviews and audits to identify any non-compliance issues and take appropriate actions to address them.
- **Customer Due Diligence (CDD):** The compliance team oversees the customer onboarding process and ensures that proper due diligence is conducted on all clients. They verify the identities of clients, assess their risk profiles, and monitor ongoing business relationships to detect any suspicious activities.
- **Training and Awareness:** The compliance team is responsible for providing training and awareness programs to employees at all levels of the organization. These programs aim to educate staff about AML/CFT regulations, red flags of suspicious transactions, and the importance of compliance in mitigating financial risks.
- **Reporting and Record-Keeping:** The compliance team prepares and submits reports on Ashkenazi Trading compliance with AML/CFT regulations to regulatory authorities as required. They also maintain records and documentation related to compliance activities, including suspicious transaction reports, risk assessments, and training records.
- **Internal Controls and Risk Assessments:** The compliance function establishes internal controls and procedures to mitigate the risk of money laundering and terrorist financing. They conduct risk assessments to identify potential vulnerabilities and develop strategies to address them effectively.
- **Collaboration and Communication:** The compliance team collaborates with government agencies, law enforcement bodies, and other organizations to share information and best practices in combating financial crimes. They also act as a point of contact for regulatory agencies and ensure timely communication and cooperation with them.
- **Continuous Improvement:** The compliance function regularly reviews and updates AML/CFT policies and procedures based on changes in regulations and emerging risks. They stay informed about industry trends, regulatory updates, and best practices to enhance the effectiveness of the compliance program.



14.3. Overall, the compliance function within Ashkenazi Trading plays a vital role in safeguarding the organization's reputation, protecting it from legal and regulatory risks, and promoting a culture of ethical conduct and integrity.

## 15. Policy Custodian

15.1. As stated, the management team of Ashkenazi Trading is designated as the custodian of the Policies and Procedures Manual for Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations. The Manager of **Ashkenazi Trading** holds the ultimate responsibility for the administration and enforcement of the policy. This means that the Manager plays a crucial role in ensuring that the AML/CFT policies and procedures are effectively implemented, followed, and enforced throughout the organization.

15.2. The specific responsibilities of the Manager may include:

- **Overall Oversight:** The General Manager is responsible for overseeing the implementation and enforcement of the AML/CFT policies and procedures. They ensure that the necessary resources, including personnel, technology, and training, are allocated to support compliance efforts.
- **Policy Administration:** The General Manager is responsible for the administration of the AML/CFT policy. This includes reviewing and approving the policy, ensuring its alignment with regulatory requirements, and making any necessary updates or amendments.
- **Leadership and Accountability:** The General Manager sets the tone from the top, emphasizing the importance of AML/CFT compliance, and fostering a culture of compliance throughout the organization. They hold the management team and employees accountable for their compliance obligations.
- **Regulatory Compliance:** The General Manager stays informed about changes in AML/CFT regulations and ensures that the company's policies and procedures are updated accordingly. They oversee the company's response to regulatory inspections or audits and work to address any findings or recommendations.
- **Training and Awareness:** The General Manager supports and promotes AML/CFT training programs for employees at all levels of the organization. They ensure that employees are adequately trained in AML/CFT requirements, reporting obligations, and the company's policies and procedures.
- **Risk Management:** The General Manager participates in the assessment and management of AML/CFT risks within the organization. They work closely with the Compliance Officer and relevant departments to identify and mitigate risks, establish internal controls, and monitor the effectiveness of risk mitigation measures.



- **Reporting and Escalation:** The General Manager ensures that appropriate reporting mechanisms are in place for suspicious activities or potential AML/CFT violations. They oversee the reporting process, including the submission of Suspicious Transaction Reports (STRs) to regulatory authorities when required.
- **Internal Coordination:** The General Manager collaborates with the Compliance Officer and other relevant stakeholders within the organization to ensure effective coordination and communication regarding AML/CFT matters. This includes addressing compliance issues, resolving conflicts, and implementing necessary corrective actions.

15.3. By assuming these responsibilities, the General Manager demonstrates their commitment to AML/CFT compliance and plays a vital role in establishing and maintaining a robust AML/CFT framework within the organization.

## 16. Periodical Review

16.1. The AML/CFT Policy of Ashkenazi Trading incorporates a regular review process to ensure its effectiveness and alignment with evolving legislative requirements. The key points regarding the policy review are as follows:

- **Annual Review:** The AML/CFT Policy shall be reviewed at least on an annual basis. This periodic review allows for a comprehensive assessment of the policy's implementation, effectiveness, and compliance with the latest legislative changes and amendments related to AML/CFT.
- **Consideration of Legislative Changes:** During the review process, particular attention will be given to any legislative changes or amendments regarding AML/CFT. The policy will be updated to incorporate these changes and ensure ongoing compliance with the applicable laws and regulations.
- **Evaluation of Implementation:** The review will also assess the previous twelve months' implementation of the AML/CFT Policy. This evaluation will examine how the policy was implemented in practice, identify areas for improvement, and determine if any challenges or gaps need to be addressed.
- **Feedback from Relevant Authorities:** Periodical checks and inspections conducted by relevant authorities may provide valuable feedback on the implementation of the AML/CFT Policy. Any comments or recommendations received during these checks will be taken into consideration during the review process.
- **Approval for Amendments:** If any amendments or changes are deemed necessary during the review, they must receive prior written sign-off from the Senior Management Team of Ashkenazi Trading. This ensures that any modifications to the policy are authorized and supported by the company's top leadership.
- **Immediate Effect:** Once approved by the Senior Management Team, any



amendments, or changes to the AML/CFT Policy will take effect immediately. This ensures that the updated policy is implemented promptly and reflects the latest requirements and best practices.

16.2. By conducting regular reviews and incorporating legislative changes, feedback from authorities, and insights from the implementation process, Ashkenazi Trading aims to maintain an effective and up-to-date AML/CFT Policy that mitigates the risk of money laundering and terrorism financing.

## 17. Compliance Internal Audit

17.1. Ashkenazi Trading recognizes the importance of an independent internal audit function to ensure the effectiveness of its AML/CFT compliance efforts. The following points outline the role and responsibilities of the internal auditor:

- **Appointment and Independence:** Ashkenazi Trading must appoint an internal auditor who is responsible for assessing the effectiveness of the AML/CFT compliance measures. The internal auditor should have the necessary AML/CFT expertise and auditing experience to perform their role effectively. It is crucial that the internal auditor operates independently and has the authority within the organization to carry out their responsibilities objectively.
- **Compliance Assessment:** The internal auditor's primary responsibility is to assess the effectiveness of the AML/CFT processes and controls within Ashkenazi Trading. This assessment includes evaluating the compliance with regulatory requirements as well as internal management requirements related to AML/CFT.
- **Identification of Weaknesses:** The internal auditor plays a key role in identifying any weaknesses or deficiencies in the AML/CFT controls. By regularly tracking and monitoring these potential weaknesses, the internal auditor contributes to the ongoing improvement of the AML/CFT processes and helps ensure their effectiveness.
- **Reporting to the AML/CFT Committee:** The internal auditor reports directly to the AML/CFT Committee, which provides oversight and coordination of the AML/CFT procedures within Ashkenazi Trading. This reporting structure ensures independence and facilitates effective communication between the internal auditor and the committee.

17.2. By appointing an independent internal auditor and ensuring their expertise and authority, Ashkenazi Trading strengthens its AML/CFT compliance efforts. The internal auditor's assessment and reporting contribute to the continuous improvement of the AML/CFT controls and help maintain regulatory compliance. The responsibilities of the internal auditor shall include:

- **Periodic Assessment of Documentation:** The internal auditor assesses the relevant



AML/CFT program documentation, such as KYC/CDD/EDD policies and procedures. This assessment helps ensure that the documentation is comprehensive, up-to-date, and aligned with regulatory requirements and industry best practices.

- **Testing of AML/CFT Controls and Processes:** The internal auditor conducts testing of the AML/CFT controls and processes implemented by the company. This testing includes evaluating the effectiveness of KYC/CDD/EDD procedures, training programs, suspicious-activity reporting mechanisms, and record-keeping practices. By conducting these tests, the internal auditor identifies any weaknesses or gaps in the controls and processes and recommends improvements.
- **Evaluation of AML/CFT Risk Assessment:** The internal auditor periodically evaluates the AML/CFT risk assessment conducted by Ashkenazi Trading. This evaluation ensures that the risk assessment is comprehensive, accurate, and reflects the evolving risk landscape. If any deficiencies or changes in risk factors are identified, the internal auditor recommends appropriate adjustments to the risk assessment.
- **Follow-up on Remedial Actions:** The internal auditor follows up on any remedial actions that arise from independent audits or regulatory findings. This includes ensuring that corrective measures are implemented in a timely manner and that they effectively address the identified deficiencies or non-compliance issues. By monitoring the implementation of remedial actions, the internal auditor helps to ensure that the AML/CFT program is continuously improved and remains in compliance with regulatory requirements.

17.3. These activities performed by the internal auditor contribute to the overall effectiveness of the AML/CFT program at Ashkenazi Trading. By conducting assessments, testing, and evaluations, and by following up on remedial actions, the internal auditor helps identify and address any weaknesses or non-compliance issues, thereby strengthening the company's AML/CFT controls and processes.

## 18. Procedure and Controls (General)

18.1. Ashkenazi Trading is required to establish and implement internal control procedures aimed at preventing and impeding money laundering, financing of terrorism and financing of illegal organizations. This Policy contains, as an integral part to it, certain procedural checks, and balances (collectively "Procedures and Controls") to ensure the vigilant and effective operation of the Policy.

18.2. Such procedures shall, among other things, ensure that all stakeholders are aware of the provisions of the law, its implementing rules, and regulations, as well as all reporting and control procedures established by Ashkenazi Trading and the supervising authority. Ashkenazi Trading shall see to it that their respective policies and procedures for dealing with AML/CFT are clearly set out and reflected in their operating manual.



18.3. The Procedures and Controls are as follows:

- Identification, Verification and KYC
- Updating KYC information
- Activity Monitoring
- Reporting of Suspicious Activities
- Training and Awareness
- Record Keeping

## 19. Identification, Verification, and Know Your Customer

- 19.1. Ashkenazi Trading has established, documented, and maintained a comprehensive Customer Identification Program that is appropriate for the size and nature of its business operations. This program will incorporate the requirements specified in the KYC Checklist, which outlines the necessary information and documents to be obtained from clients.
- 19.2. As part of the Customer Identification Program, Ashkenazi Trading is committed to obtaining and recording competent evidence of the true and full identity of its clients, including their Ultimate Beneficiary Owners, representatives, domicile, legal capacity, occupation, business purposes, and other relevant identifying information. The documents detailed in the KYC Checklist will be utilized for this purpose.
- 19.3. Upon conducting applicant screening, background checks, and reviewing the client's business plan, source of funds, and expected activity levels, an initial decision will be made regarding the application status. This decision may involve acceptance, rejection, or the request for additional information.
- 19.4. Ashkenazi Trading communicates to its clients that business transactions will not be conducted with applicants who fail to provide competent evidence of their activities and identity. However, it is important to note that Ashkenazi Trading maintains its legal and ethical obligation to report any suspicious transactions, irrespective of the client's provision of evidence.
- 19.5. In cases where initial verification fails to identify the applicant or raises suspicions about the provided information, Ashkenazi Trading will undertake additional verification measures. These measures are designed to ensure the accuracy and integrity of the information and help determine whether to proceed with the business transaction. Detailed records of the additional verifications conducted will be maintained.



- 19.6. By adhering to these ID, VR, and KYC procedures, Ashkenazi Trading demonstrates its commitment to preventing money laundering, financing of terrorism, and other illicit activities, while also fulfilling its legal obligations and safeguarding its reputation.
- 19.7. In situations where Ashkenazi Trading has reasons to doubt the accuracy of information pertaining to the customer's identity, the customer's status as the beneficial owner, the intermediary's declaration of beneficial ownership, or if there are any indications of unreported changes, further measures will be taken to verify the identity of the customer or beneficial owner, as applicable.
- 19.8. These measures are aimed at ensuring the integrity of the customer identification process and mitigating the risk of illicit activities. The specific actions that may be taken by Ashkenazi Trading in such cases include:
- **Referral of names and other identifying information to criminal investigating authorities:** Ashkenazi Trading may share the relevant information with appropriate law enforcement or regulatory authorities for further investigation. This step helps in confirming the accuracy of the information and addressing any potential suspicions or concerns.
  - **Review of disciplinary history and disclosure of past relevant sanctions:** Ashkenazi Trading will examine previous instances of non-compliance, regulatory violations, or any other relevant misconduct. Such a review helps in assessing the customer's credibility and determining the level of risk associated with the business relationship.
- 19.9. The Customer Identification Program includes procedures for responding to circumstances in which the Compliance Monitoring Team cannot form a reasonable belief that it knows the identity of a customer. These procedures should describe, among others, the following:
- When Ashkenazi Trading should not do business with a client.
  - The terms under which a customer may conduct business transactions while Ashkenazi Trading attempts to verify the customer's identity.
  - When Ashkenazi Trading should file a Suspicious Activities / Transaction Report.
- 19.10. The Customer Identification Program must include procedures for providing customers adequate notice that Ashkenazi Trading is requesting information to verify their identities.
- 19.11. In rare events or incidences where a Customer fails to provide adequate KYC information or appears hesitant/unwilling to provide information as required to establish adherence to KYC norms, Ashkenazi Trading shall not proceed with a transaction for such as Customer and flag the case as a High-Risk customer. Such cases are marked for reporting to the Regulator through Suspicious Transaction Report (STR), and for increased monitoring.



## 20. Risk-Based Approach

- 20.1. A risk-based approach is one of the most effective ways to protect against money laundering and terrorist financing. It is imperative to understand that certain risks associated with various elements of a customer's profile may be indicative of potential criminal activity. This may include geographical and jurisdictional issues, business and product types, distribution channels and prevailing transaction types and amounts.
- 20.2. Customers will be reviewed, assessed, and allocated an appropriate level of risk of money laundering, divided into – High, Medium or Low Risk.
- **High** risk customers will be subject to enhanced levels of due diligence that go beyond the core policies and principles contained in this policy.
  - **Medium** risk customers will be subject to the core policies and procedures contained within this policy.
  - **Low** risk customers may be subject to a certain flexibility within the policies and procedures contained within this policy. However, great care should be exercised to ensure that the Company continues to meet its legal obligations.
- 20.3. While it is generally understood that failure to provide satisfactory due diligence documentation may raise concerns about money laundering, it is also acknowledged that due to the diverse nature of businesses, obtaining documentation that precisely meets the criteria outlined in this policy may sometimes be challenging or even impossible.
- 20.4. In cases where it is difficult to obtain the required documentation but there are no suspicions of money laundering, the customer's documentation should be forwarded to senior management and/or the Compliance Officer. Along with the documentation, an explanation should be provided, outlining the specific issues that arose. Senior management, in consultation with the Compliance Officer, will then review the documentation and assess the risks associated with accepting identification evidence that falls outside the established procedures. They will provide appropriate guidance and advice to the personnel involved.
- 20.5. The assessment process, decision-making, and the resulting conclusions should be thoroughly documented in the customer's KYC file. The individuals involved in the review should provide their sign-off. Only Senior Management, in consultation with the Compliance Officer, have the authority to determine the level of risk attributed to a customer and approve documentation that does not fully meet the exact requirements specified in the company's anti-money laundering policy.



- 20.6. All customers are subject to a risk assessment and the risk ratings will be recorded in the file. Due diligence requirements must be commensurate with the risk level associated with the customer and EDD will be necessary for all higher risk customers.
- 20.7. In addition to trigger-based reviews, Ashkenazi Trading shall conduct periodic review of Customer's KYC and conduct CDD based on the risk profile of the customer:
- **High Risk Customers:** Every 12 months
  - **Medium Risk Customers:** Every 18 months
  - **Low Risk Customers:** Every 24 months
- 20.8. When dealing with customers who have not triggered any alerts, Ashkenazi Trading has the option to refresh the necessary information and perform simplified due diligence. This involves requesting customers to confirm the baseline information already on file and provide supporting documentation.
- 20.9. For customers who have triggered an alert, a more thorough assessment and review of their activities may be necessary.
- 20.10. In addition to assessing the risks associated with onboarding customers, Ashkenazi Trading is also required to conduct its own internal risk assessment. This assessment should not only consider the inherent risks related to the company's sector but also include potential risk factors beyond its specific industry and internal operations. The findings of this assessment should be submitted to Senior Management and should include recommendations for mitigating such risks. The report on the internal risk assessment has been prepared separately and is attached as an annex to this policy.

## 21. KYC Process

- 21.1. Ashkenazi Trading maintains clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk. Before accepting a client, KYC and due diligence procedure are followed, by examining factors such as customers' background, country of origin, public or high-profile position, business activities or other risk indicators.
- 21.2. KYC is to be carried out according to mandatory Customer KYC checklist:
- Natural Person and Individual Members of Corporate Client KYC Checklist (Refer to Appendix A)
  - Legal Person (Corporate) KYC Checklist (Refer to Appendix B)
- 21.3. Ashkenazi Trading should be required to conduct KYC and CDD procedure when:



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

21.4. If the customer is unable to comply with these requirements, Ashkenazi Trading should:

- Not open the account, commence business relations, or perform the transaction.
- Terminate the business relationship.
- Consider filing a suspicious-transaction report in relation to the customer.

21.5. Ashkenazi Trading is strictly forbidden to do business with shell companies. Shell companies meaning, an institution that has no physical presence in any country, no active business, merely exists on paper.

21.6. An integral part of the KYC process is the carrying out customers screenings and relative risk assessments. Screening ensures that a customer is not listed on the official sanctions' lists issued by Government and law enforcement agencies. Background checking is designed to identify any adverse information about the past conduct of an individual that may influence their suitability as a customer.

21.7. When conducting the KYC process, there shall be no reliance on third party information or "hearsay". For applicants introduced to Ashkenazi Trading by a third party, Ashkenazi Trading must carry out and perform all identification, verification, and KYC procedures.

21.8. It should be borne in mind that KYC is more than a procedure and is a discipline that is to be developed. For example, KYC should become second nature so that any significant information related to the customer obtained during meetings, telephone discussion, visits, online search, etc. and is deemed to be relevant for the purposes of the Policy should be recorded. Fresh due diligence should be undertaken, especially if it appears that the veracity or accuracy of previous information is doubted.

## 22. Customer Onboarding

22.1. In general, Ashkenazi Trading will have the following as its customers:



- Natural persons; and
- Legal persons, including individual members of corporates.

*Natural Persons and Individual Members of Corporate Customers*

22.2. Ashkenazi Trading shall obtain from all individual members of corporate customers, including shareholders, beneficial owners, directors, managers, authorized signatories, power of attorney holders, and other key managerial people, the following information:

- Individual's full name (as per passport)
- Date and place of birth
- Nationality
- Passport Number
- National Identity Document (Emirates ID, for UAE nationals / resident)
- Physical Address (residential and business / home country and UAE)
- Contact details.
- Source of funds and wealth
- Declaration regarding Beneficial Ownership, that is, the person who has the ultimate ownership.
- Whether the customer is a Politically Exposed Person (PEP) or Close Associate of a PEP

The above list is a summary of the information required. A detailed checklist is attached in Appendix A.

22.3. As part of the process for identifying and verifying customers, and for authenticating the original documents upon which the verification is based, Ashkenazi Trading will include procedures for the certification of the customer identification and address documentation it obtains. Ashkenazi Trading shall request members of corporate clients to produce or show the original documents for verification purposes. Such procedures will encompass:

- Certification by employees (for example, by including the name, title of position, date, and signature of the verifying employee(s) on the copies of documents maintained on file, along with a statement representing that the copy of the document is a "true copy of the original") and/or,
- third parties (for example, by including the name, organization, title of position, date, and signature of the verifying person, along with a statement representing that the copy of the document is a "true copy of the original").



22.4. If physical verification is not possible, or the customer is not in the UAE, Ashkenazi Trading staff may do the verification of original ID on a secured video platform such as Zoom or Google Meet and store a screenshot as evidence of verification.

22.5. For individual, in case the original ID documents cannot be presented for verification, a duly authenticated document by the UAE Embassy in the home country of the individual or duly attested documents by UAE Notary Public in case the individual is in the UAE can be acceptable in place of the original documents. In cases where documents are obtained from foreign sources in countries which are members of the Hague Apostille Convention, Ashkenazi Trading may request documents certified by Apostille seal.

#### Legal Persons

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

22.7. Ashkenazi Trading shall obtain from all corporate customers the following information:

- Incorporated name
- Shareholders (To include 'active', 'silent' and/ or 'sleeping' partners)
- Ultimate beneficial owners (the Beneficial Owner shall be whomever that ultimately owns or controls, whether directly through a chain of ownership or control or by other means of control such as the right to appoint or dismiss most of its Directors, owning 25% or more of the shares or 25% or more of the voting rights in the Legal Person)
- Managers (That person having the day-to-day control of the company if not a shareholder/partner)
- Authorized Signatories
- Passport of All shareholders, Ultimate beneficial owners, Managers, Signatories
- National Identity Document of shareholders, Ultimate Beneficial Owners, Managers, Signatories (Emirates ID, if a customer is a resident/citizen of UAE).
- Memorandum and Articles of Association.
- Power of Attorney (if applicable).
- Proof of physical address of the company and UBO/Shareholder
- Contact details.



- Business activities (type and volume)
- Source of funds and wealth

The above list is a summary of the information required. A detailed checklist is attached in Appendix B.

22.8. As part of the process for identifying and verifying customers, and for authenticating the original documents upon which the verification is based, Ashkenazi Trading will include procedures for the certification of the customer identification and address documentation it obtains. Ashkenazi Trading shall request corporate clients to produce or show the original documents for verification purposes. Such procedures will encompass:

- Certification by employees (for example, by including the name, title of position, date, and signature of the verifying employee(s) on the copies of documents maintained on file, along with a statement representing that the copy of the document is a “true copy of the original”) and/or,
- third parties (for example, by including the name, organization, title of position, date, and signature of the verifying person, along with a statement representing that the copy of the document is a “true copy of the original”).

22.9. If physical verification is not possible, or the customer is not in the UAE, Ashkenazi Trading staff may do the verification of original ID on a secured video platform such as Zoom or Google Meet and store a screenshot as evidence of verification.

22.10. For companies or businesses, in case the original ID documents are not available, a duly authenticated document by the UAE Embassy in the home country of the Company or duly attested documents by UAE Notary Public in case the Company is in the UAE can be acceptable in place of the original documents. In cases where documents are obtained from foreign sources in countries which are members of the Hague Apostille Convention, Ashkenazi Trading may request documents certified by Apostille seal.

22.11. Ashkenazi Trading shall take additional care in dealing with cases where customer verification is done without face-to-face contact with the ultimate client for corporate customers.

## 23. Customer Due Diligence

23.1. Customer Due Diligence (CDD) is a critical process in the DPMS (Dealers in Precious Metals and Stones) sector to combat money laundering and terrorist financing. It involves gathering and verifying relevant information about customers to evaluate their identity, background, and associated risks. The primary objective of CDD in the DPMS sector is to



prevent and detect illicit activities, ensure compliance with regulations, and protect businesses from potential risks.

23.2. Due to the unique characteristics of the DPMS sector, monitoring customer activities and transactions on an ongoing basis can be challenging. DPMS businesses, including dealers in precious metals and stones, must place particular emphasis on the effectiveness of their CDD measures to address the specific risks within their industry.

23.3. By conducting thorough and comprehensive CDD, DPMS businesses can better understand their customers, identify potential risks, and take appropriate measures to mitigate those risks. This includes implementing appropriate and proportionate CDD measures tailored to the DPMS sector and continuously monitoring customer relationships and transactions.

23.4. DPMS businesses should adapt their CDD processes to account for the transactional nature of the industry, the involvement of different parties, and the need for ongoing monitoring. This may involve:

- Gathering and verifying customer information, including identification documents, trade licenses of entities, and identification documents of local representatives.
- Assessing the identity, background, and associated risks of customers in order to evaluate their suitability for engaging in DPMS transactions.
- Conducting ongoing supervision of customer activity and auditing transactions to ensure consistency with customer information, types of activity, and risk profiles.
- Investigating and obtaining additional information for high-risk customers or business relationships to understand the purpose of transactions and enhance monitoring for unusual or suspicious activities.
- Evaluating the specifics of transactions in relation to customer profiles and obtaining sufficient information on counterparties and other involved parties to determine if the transactions are normal, reasonable, and legitimate.
- Continuously adapting and improving CDD measures to address evolving risks and regulatory requirements in the DPMS sector.

23.5. CDD should be conducted at the onset of the business relationship and throughout its duration. It is an ongoing process that helps businesses mitigate risks, comply with AML/CTF regulations, and contribute to the overall integrity of the financial system.

## 24. Enhanced Due Diligence

24.1. A High-Risk Customer will be one who presents a higher-than-normal adverse potential risk of involvement in money laundering or financing of terrorism or financing of illegal



organization or any other matter that Senior Management or the Chief Compliance Officer consider to be significant.

24.2. To mitigate the increased risks associated with the High-Risk Customers, it will be necessary to consider the application of a level of enhanced due diligence for those customers. Ashkenazi Trading' Senior Management, in consultation with the Chief Compliance Officer, will determine whether the level of risk is acceptable.

24.3. Enhanced Due Diligence ("EDD") will need to go beyond the normal requirements applied to the approval and monitoring of customers, as contained within this policy. As the reasons for designation as high risk will vary from customer to customer, the nature and level of enhancement will need to be determined separately as and when high risk customers are identified.

24.4. To perform EDD on their customers, the additional documents that may be required to be collected by Ashkenazi Trading for the High-Risk Customer may include, but not limited to, the following:

- Audited Financial Statement
- Tax Return
- Bank Statements
- AML/CFT Policy
- Bank Reference Letter
- Dubai Good Delivery / LBMA / RJC Certificates
- Independent Assurance Report
- Business Profile

24.5. The above-mentioned additional documents, if collected in full or partially, will assist the team to perform further checks to identify controls within the client organization to help gauge the risk and obtain a comfort on engaging with such client.

24.6. In case Ashkenazi Trading is not satisfied with the mitigating controls identified during the EDD, the customer will be rejected and will not be onboarded.

24.7. All High-Risk customer files must be approved by Senior Management. Ashkenazi Trading shall perform Enhanced Due Diligence in the following scenarios:

- Customer entities incorporated in High-risk countries.
- Politically Exposed Persons (PEPs) and Close Associates of PEPs.
- If the customer/transaction is found to be suspicious/unusual.



- Any other suspicious cases alerted based on the rule violation(s).

24.8. The above scenarios are reviewed periodically and updated as required through the Quarterly Compliance Committee Meeting.

## 25. Politically Exposed Persons

25.1. A Politically Exposed Person or PEP is a term that is used to describe individuals who are, or have been entrusted with prominent public positions, that can be susceptible to bribery and corruption. The following list contains examples of persons who may be considered PEPs, although this list should not be viewed as exhaustive:

- Current and Ex – Head & Deputy Head of state or National Government (President, Prime Minister, Government Ministers, Provincial Governors, Cabinet Members their Deputies (assistants), Senior Ministerial staff, and Secretaries.
- Current and ex-Members of National and Provincial Assemblies and Senate.
- Senior Civil Servants including Senior Government Officials, Heads of Government Departments, and Police Service.
- Senior Judicial & Military officials
- Senior Executives of state-owned Corporations.
- High ranking Officers in Diplomatic Service (Ambassadors, High Commissioners, Envoys, Attachés, Consul Generals, Consuls, Honorary Consuls, Counsellors etc.)
- Senior Political Party Officials and functionaries such as Leader, Chairman, Deputy leader, Secretary General, and Executive Committee or any other Senior ranks in party (does not include middle ranking or more junior individuals).
- Close family members of PEPs include spouses, children, parents, siblings and may also include other blood relatives and relatives by marriage.
- Associated persons including close business colleagues and personal Advisors / Consultants to the politically exposed person as well as persons who are expected to benefit significantly by being close to such a person.

25.2. PEPs, or Politically Exposed Persons, hold positions of power and influence that can potentially be exploited for committing money laundering, corruption, bribery, and other illicit activities. They may also unwittingly have their public position used for illegal activities. The risk associated with PEPs is significantly heightened when they are in high-risk countries.

25.3. To mitigate the risks associated with PEPs, Ashkenazi Trading will ensure that each underlying beneficial owner or controller is not a PEP. This will be achieved by conducting searches on official national and international databases to screen names against



Ashkenazi Trading database or by referring to publicly available information. The results of these verifications will be documented and recorded within the customer's KYC file.

25.4. By implementing these measures, Ashkenazi Trading aims to prevent the involvement of PEPs in money laundering, terrorist financing, corruption, and other illicit activities, and to ensure compliance with regulatory requirements.

25.5. If a PEP is identified, Ashkenazi Trading will:

- Assign a rating of high-risk to the customer.
- Complete a PEP Report, ensuring that the Head of AML/CFT Committee approves establishing a business with the customer.
- Conduct EDD and be vigilant in monitoring the business relationship.
- Ensure reasonable measures will be taken to establish sources of wealth and sources of funds.
- Track PEP relationships for the purposes of reporting and monitoring.

25.6. In addition, the Compliance Officer is required to maintain a separate record/register of all PEP customers with whom Ashkenazi Trading has done the business with and the approval of such transactions from Senior Management/Head of AML/CFT Committee is also to be documented in a separate record.

## 26. Sanctioned Individuals/Entities

26.1. Ashkenazi Trading 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)

26.2. 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).

26.3. Ashkenazi Trading 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 of funds in accordance with Section 22 on TFS.



## 27. Updating KYC Information

- 27.1. 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.
- 27.2. KYC information is crucial for effective CDD and ongoing monitoring. Ashkenazi Trading 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.
- 27.3. As a minimum standard, Ashkenazi Trading 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.
- 27.4. By regularly updating KYC information, Ashkenazi Trading 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.

## 28. Monitoring of Client's Activities

- 28.1. In line with regulatory requirements, Ashkenazi Trading 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 provided information, stated activities, and risk profiles.
- 28.2. For customers or business relationships identified as high risk, Ashkenazi Trading 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.
- 28.3. Considering the level of risk involved, Ashkenazi Trading 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 authorizations.

28.4. By conducting thorough evaluations and obtaining relevant information, Ashkenazi Trading 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.

## 29. Indicators of Suspicious Activities – Red Flags

29.1. Criminals continuously adapt their methods for conducting money laundering, financing of terrorism, and financing illegal organizations. 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.

29.2. 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 the Ashkenazi Trading Owner/Manager to make an appropriate determination as to whether the transaction should be regarded as suspicious or not.

29.3. 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.



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

- Suddenly cancels 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 provided information.
- 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 organization 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 Ashkenazi Trading.
- Is located a significant distance away from Ashkenazi Trading 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.
- Makes unusual requests, including those related to secrecy, to Ashkenazi Trading or its employees.
- Is willing to pay significantly higher fees without legitimate reasons.
- Appears 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 authorization 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 or frequency 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.

29.5. 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.
- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys).



- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g., it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties:
  - Do not show particular interest in the details of the transaction.
  - Do not seem particularly interested in obtaining a better price for the transaction.
  - 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).

29.6. 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.

### 30. Targeted Financial Sanctions (TFS)

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

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

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

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

- All DNFBPs, including Dealers in Precious Metals and Stones are obliged by UAE law to apply policies, procedures, and controls to implement TFS to those sanctioned and designated in the UAE Local Terrorist List & UN Consolidated List (Sanctions List).

#### Purpose of Targeted Financial Sanctions

30.4. The purpose is to simply deny certain individuals, entities, or groups the means to violate international peace and security, support terrorism or finance the proliferation of weapons of mass destruction and further to ensure that no funds or other assets or services of any kind are made available.

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



- Terrorism and Terrorist Financing
- The Proliferation of Weapons of Mass Destruction (WMS)
- Other UN Sanctions Regimes with TFS

#### Updated Sanctions Lists

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

- The UAE has a Local Terrorist List of all the sanctioned individuals, entities, or groups designated by the UAE Cabinet. The link to the Local Terrorist List can be found at the bottom of the Sanctions Implementation webpage on the Executive Office's website: <https://www.uaieic.gov.ae/en-us/un-page?p=2#>.
- The UNSCC has a UN consolidated List of all the sanctioned individuals, entities or groups designated by the United Nations Sanctions Committees or directly by the UNSC. This link can be found on: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

30.7. The measures including the asset freezing and prohibition to offer funds and services prescribed under the policies, procedures and controls regulating the Targeted Financial, apply to:

- a. Any individual, group, or entity listed in the Local Terrorist List defined by the Federal Cabinet or listed by the UNSC in its Consolidated Sanctions List.
- b. Any entity, directly or indirectly owned or controlled by an individual or entity listed under a.
- c. Any individual or entity acting on behalf of or in the direction of any individual or Entity listed under a & b.

30.8. There is no time limit prescribed for asset freezing, and prohibition measures. The regulations provide that the funds will remain frozen, and the prohibition to offer funds and services stands until the individual, group, or entity is removed from the Local Terrorist List or the UN List or until there is a freezing cancellation decision made by a competent authority or the UNSC.

### 31. TFS Obligations

31.1. TFS must be implemented in accordance with the relevant UNSC Resolutions, including the UN Consolidated List, and the Local Terrorist List.

31.2. There are four main obligations to implement TFS:



### 31.3. **Step 1 – Subscribe**

- Ashkenazi Trading is required to subscribe to the EOCN Notification System on the EOCN's website to receive automated email notifications on any updates to the Sanctions Lists: <https://www.uaieic.gov.ae/en-us/un-page>.
- This registration is aimed at helping Ashkenazi Trading to receive updated and timely information about the designation and de-listing of individuals, entities, or groups in the Sanctions Lists.

### 31.4. **Step 2 – Screen**

- Ashkenazi Trading must undertake regular and ongoing screen on the latest Local Terrorist List and UN Consolidated List.
- Screening must be undertaken under following circumstances:
  - Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
  - Prior to onboarding new customers.
  - Upon KYC reviews or changes to a customer's information.
  - Before processing any transaction.
- There are three types of screening results which are as follows:
  - Potential Match – A potential match is when there is a partial match between the identities in the Sanctions Lists and any information in the database and it is not possible to conclude a false-positive or a confirmed match.
  - Confirmed Match – A confirmed match is when an individual, entity, or group matches all the key identities published on the Sanctions List.
  - False-Positive Result – A false-positive is a potential match to listed individuals, entities, or groups, either due to the common nature of the name or due to ambiguous identifying data, which on examination proves not to be a confirmed match.

### 31.5. **Step 3 – Apply TFS**

31.5.1. The following are the TFS measures that must be implemented if a match with the Local Terrorist List or UN Consolidated List is identified.

31.5.2. **Freeze all funds or other assets without delay:** Freeze without delay (immediately or in any case within 24 hours) and without prior notice to the designated individual, entity, or group, all the funds or other assets:

- a. Owned or controlled, wholly or jointly, directly, or indirectly, by an individual, entity, or



group designated in the Local Terrorist List or the UN Consolidated List.

- b. Derived or generated from funds or other assets under item a, or
- c. Any individual or entity acting on behalf of or at the direction of any designated individual, entity, or group.

31.5.3. The obligations to freeze without delay shall not prevent additions to frozen accounts of:

- a. Interest, profits, or other earnings due on the account; or
- b. Of payments due under contracts, agreements or obligations agreed upon prior to the date on which the account has become subject to freezing, provided such additions are immediately frozen.

31.5.4. **Prohibition of making funds or other assets or services available:** DNFBPs are prohibited from providing funds or other assets to or rendering financial services or other services related to, whether in whole or in part, directly or indirectly, or for the benefit of, any designated individual, entity, or group on the Local Terrorist List or on the UN Consolidated List.

#### 31.6. **Step 4 – Report**

31.6.1. Report any freezing or suspension measures taken upon identifying confirmed or potential matches through the goAML platform.

#### Additional Obligations for Ashkenazi Trading

31.7. In addition to the above, Ashkenazi Trading must also fulfil the following obligations:

- Cooperate with the EOCN and the relevant Supervisory Authority in verifying the accuracy of the submitted information.
- Implement the freezing, cancellation, or lifting decision, when appropriate, without delay, pursuant to related UNSCRs or decisions of the Cabinet regarding issuance of the Local Terrorist List.
- Set and implement policies, procedures, and internal controls to:
  - Ensure compliance with the obligations arising from Cabinet Decision No. 74 of 2020.
  - Identify the existing accounts, transactions, funds or other assets of designated individuals, entities, or groups.
  - Conduct ongoing TFS training and awareness sessions to relevant employees and senior management.
  - Adopt reasonable measures to consider beneficial owners, signatories, and



powers of attorney with respect to accounts or transactions held by Ashkenazi Trading when searching for activities by designated individuals, entities, or groups.

- Prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action or any Other Measures are going to be implemented as per provisions of Cabinet Decision No. 74 of 2020.
- Ensure having the appropriate resources to meet the obligations of implementing TFS.

31.8. Failure by Ashkenazi Trading to comply with the obligations outlined in Cabinet Decision No. 74 of 2020 or to implement appropriate compliance procedures may result in legal consequences. The company may be subject to imprisonment ranging from one to seven years and/or a fine ranging from AED 50,000 to AED 5,000,000.

31.9. Furthermore, Ashkenazi Trading is subject to supervision by the Supervisory Authorities. In cases of identified non-compliance, the Supervisory Authorities have the authority to apply enforcement actions as specified in Article 14 of Federal Decree No. 26 of 2021, which amends certain provisions of Law No. 20 for 2018 on Anti-Money Laundering and Countering the Financing of Terrorism. The Supervisory Authorities are legally empowered to oversee the implementation of measures to combat money laundering and terrorist financing.

31.10. In addition to the legal consequences mentioned earlier, the Supervisory Authorities could impose various administrative sanctions on Ashkenazi Trading for non-compliance. These sanctions may include:

- Issuing a letter of warning.
- Imposing administrative penalties ranging from AED 50,000 to AED 5,000,000 for each violation.
- Banning the violator from working in the sector related to the violation for a specified period determined by the Supervisory Authority.
- Imposing constraints on the powers of board members, supervisory or executive management members, managers, or owners who are found to be responsible for the violation. This may include the appointment of a temporary inspector.
- Suspending managers, board members, and supervisory and executive management members who are proven to be responsible for the violation for a period determined by the Supervisory Authority or requesting their removal.
- Suspending or restricting the activity or profession of Ashkenazi Trading for a period determined by the Supervisory Authority.
- Cancelling the license of Ashkenazi Trading.



31.11. These administrative sanctions serve as additional measures to ensure compliance with the regulations and to address any violations identified by the Supervisory Authorities.

31.12. Any Entity that acts in good faith and complies with the provisions of Cabinet Decision No. 74 of 2020 by freezing funds or other assets, denying disposal thereof, refusing to provide financial services to designated individuals, entities, or groups, or declining to perform any other obligation (including reporting obligations), shall be exempt from any damages or claims. This exemption applies to any penal, civil, and/or administrative liability that may arise because of such actions.

## 32. Ongoing Screening

32.1. To ensure compliance with the changing TFS restrictions, it is the responsibility of all Ashkenazi Trading to establish and maintain appropriate controls and procedures. These measures are necessary to effectively implement the TFS restrictions and mitigate the risk of engaging in financial transactions with individuals or entities listed on the Local Terrorist List and UN Consolidated List.

32.2. Ashkenazi Trading is required to screen against the latest versions of the Local Terrorist List and UN Consolidated List regularly and consistently. This screening should be conducted at key stages, including prior to onboarding new customers, during periodic KYC reviews or when there are changes to a customer's information, and before processing any transactions.

32.3. By conducting regular screenings and keeping up to date with the latest lists, Ashkenazi Trading can ensure that they are not involved in any prohibited financial activities or transactions with individuals or entities subject to TFS. It is crucial to maintain accurate and current controls to effectively implement the TFS restrictions and remain compliant with regulatory obligations.

32.4. The following databases must be included in the screening process:

- Existing customer databases: All systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance.
- Potential customers before conducting any transactions or entering a business relationship with any Person.
- Names of parties to any transactions (e.g., buyer, seller, agent, freight forwarder, etc.)
- Ultimate beneficial owners, both natural and legal.
- Names of individuals, entities, or groups with direct or indirect relationships with them.



- Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

### 33. Reporting of Suspicious Activities/Transactions

- 33.1. Ashkenazi Trading is committed to adhering to the UAE's Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) legislative and regulatory framework. As part of this commitment, the company will establish a system for mandatory reporting of suspicious transactions in accordance with the prescribed requirements.
- 33.2. If any suspicious activities or transactions are identified, they will be reported to the Financial Intelligence Unit (FIU) through the designated GoAML system. The Manager will review the matter and, if sufficient evidence is available, promptly report it to the FIU as a Suspicious Activity.
- 33.3. In cases where there are reasonable grounds to suspect that a customer has engaged in unlawful activities, the Manager will evaluate the situation and, if warranted, immediately report the case to the FIU.
- 33.4. Ashkenazi Trading will maintain a register of all suspicious transactions, including those that are reported to the FIU and those that are not. The company acknowledges that the failure to report a suspicious transaction, whether intentionally or due to gross negligence, is considered a federal crime. Any individual who fails to fulfil their legal obligation to report suspicions of money laundering, financing of terrorism, or financing of illegal organizations may face penalties, including fines and/or imprisonment.
- 33.5. To file suspicious activities/transactions (SARs/STRs) effectively, Ashkenazi Trading should follow the following procedure:
- **Collect all relevant documents:** Gather all the necessary documents related to the suspicious activity or transaction. This may include identification documents, purchase or sales transaction details, risk assessment reports, and screening reports.
  - **Log in to the FIU portal via goAML:** Access the designated goAML portal provided by the Financial Intelligence Unit (FIU).
  - **Select the type of reporting:** Within the goAML portal, choose the appropriate reporting option that corresponds to the nature of the suspicious activity or transaction being reported.
  - **Fill in the required information:** Complete all the mandatory fields in the reporting form as per the provided format. This may include details such as the nature of the suspicious activity, individuals or entities involved, transaction amounts, dates, and any other relevant information.



- **Upload the relevant documents:** Attach the collected documents to the report as supporting evidence. Ensure that all necessary files are properly uploaded and attached to the submission.
- **Submit the report:** Once all the required information and documents have been provided, submit the report through the goAML portal. Verify that the submission has been successfully made and retain a copy of the confirmation for record-keeping purposes.

33.6. By following this procedure, Ashkenazi Trading can ensure that suspicious activities or transactions are promptly reported to the appropriate authorities, facilitating the investigation and mitigation of potential financial crimes.

#### 34. Dealers in Precious Metals and Stones Report (DPMSR)

34.1. In addition to the due diligence and reporting requirements mentioned in other sections of this policy, Ashkenazi Trading, 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.

#### 35. Process of Submitting TFS Report

35.1. With regards to Ashkenazi Trading obligations for TFS reporting as stipulated in the AML/CFT law and the TFS law, the MOE in coordination with the Executive Office - IEC Circular No. 05 of 2021 has developed a unified mechanism to report TFS obligations utilizing the FIU's online reporting platform GoAML.

35.2. The FIU, in collaboration with the EOCN, has enhanced the goAML platform to allow Ashkenazi Trading to report freezing measures taken to implement TFS. The FIU has developed namely two additional reports:



- Funds Freeze Report (FFR)
- Partial Name Match Report (PNMR).

35.3. Once the reporting entity raises the FFR or PNMR through goAML, the EOCN and the relevant Supervisory Authority are notified at the same time.

35.4. ***In case a confirmed match is identified***, Ashkenazi Trading must freeze without delay (within 24hrs) all funds and other assets and submit a 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.

35.5. The following information is obligatory when submitting a Funds Freeze Report (FFR):

- **The full name of the 'confirmed match'** - Attach ID documents of the 'confirmed match,' such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.
- **Amount of funds or other assets frozen** (e.g., value of funds in bank accounts, value of transactions, value of securities, transaction value, etc.) - Attach proof documents such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.

35.6. ***In case a potential 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 PNMR through GoAML, which will be received by the Executive Office and the relevant Supervisory Authority.

35.7. The reporting entity must ensure 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').

35.8. The following information is obligatory when submitting a ***Partial Name Match Report (PNMR)***:

- **The full name of the 'potential match'** - Attach ID documents of the 'potential match,' such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.
- **Amount of funds or other assets suspended** (e.g., value of funds in bank accounts, value of transactions, value of securities, transaction value, etc.) - Attach documentary proof such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.



35.9. The MOE for the procedures on TFS reporting via the GoAML platform stipulates as below:

- When a **'confirmed match'** to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, Ashkenazi Trading is required to take the following necessary actions:
  - Implement all necessary measures without delay as outlined in the TFS law.
  - Report any freezing measure, prohibition to provide funds or services, and any attempted transactions to the MOE and the Executive Office – IEC via the GoAML platform within two business days by selecting the Fund Freeze Report (FFR).
  - Ensure all the necessary information and documents regarding the 'confirmed match' is submitted along with the Fund Freeze Report (FFR).
  - Uphold freezing measures related to the 'confirmed match' until further instructions are received from Executive Office – IEC, and
  - Notify and share a copy of the report with the Ministry of Economy through this email: [sanctions@economy.ae](mailto:sanctions@economy.ae).
- When a **'potential match'** to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, Ashkenazi Trading is required to take the following necessary actions:
  - Suspend without delay any transaction and refrain from offering any funds or services, as outlined in the guidance on TFS, and guidance for licensed DNFBPs on the Implementation of TFS.
  - Report the 'potential match' to the MOE and the Executive Office – IEC via the GoAML platform by selecting the Partial Name Match Report (PNMR).
  - Ensure all the necessary information and documents regarding the name match is submitted.
  - Uphold suspension measures related to the 'potential match' until further instructions are received from Executive Office – IEC via the GoAML platform on whether to cancel the suspension or implement freezing measures, and
- Notify and share a copy of the report with the Ministry of Economy through this email [sanctions@economy.ae](mailto:sanctions@economy.ae).

35.10. In case Ashkenazi Trading receives an email from EOCN regarding updated in Sanctions lists, then Ashkenazi Trading must undertake rescreening exercise and keep a record of the ongoing screenings done.



## 36. Tipping Off and Confidentiality

- 36.1. 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.
- 36.2. 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.
- 36.3. Ashkenazi Trading 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.
- 36.4. It is essential for Ashkenazi Trading to maintain the confidentiality of information related to suspicious transactions and investigations to ensure the effectiveness of anti-money laundering and counter-terrorist financing efforts.

## 37. Training and Awareness

- 37.1. Ashkenazi Trading recognizes the importance of education and training in promoting a strong anti-money laundering (AML) and counter-terrorism financing (CTF) culture within the organization. To fulfil this commitment, the following measures will be implemented:
- **Education and Training:** Ashkenazi Trading will provide comprehensive education and training programs to all staff members, including directors and officers, to ensure they are fully aware of their personal obligations and responsibilities in combating money laundering, financing of terrorism and illegal organizations. The training will also familiarize them with the reporting and investigation procedures in place for suspicious activities. The training programs will be designed to meet the specific needs and roles of the employees, ensuring they have the necessary knowledge and skills to fulfil their duties effectively.
  - **Assignment of Compliance Officer, Internal Audit, or Training:** Given the scale and nature of operations, Ashkenazi Trading may assign the role of Compliance Officer, Internal Audit, or Training to a competent person or professional company. The selected individual or company must have relevant experience and expertise in the field of AML/CFT. Their credentials will be validated to ensure they possess the necessary skills and knowledge to perform their duties effectively.
  - **Refresher Training:** Ashkenazi Trading will arrange for refresher trainings at least once a year to remind key staff and officers of their AML/CFT responsibilities and to update



them on any changes in national and international laws and rules related to AML/CFT. This training will help keep employees informed and ensure their knowledge is up to date.

- **Training for New Employees:** New employees will receive appropriate AML/CFT training within 30 days of their joining date. The training will cover not only the legal elements of AML/CFT laws and regulations but also job-specific applications of these laws. This will help integrate AML/CFT principles into their roles from the beginning.
- **Ongoing Training and Updates:** Ashkenazi Trading will provide ongoing training to employees to reflect current developments and changes in AML/CFT laws and regulations. Regular updates will be provided to ensure employees stay informed about evolving best practices and compliance requirements.
- **Acknowledgment of Compliance Policy:** To ensure continued adherence to Ashkenazi Trading AML/CFT and KYC policies and procedures, all employees will be required to confirm their awareness of the contents of the Compliance Policy by signing an acknowledgment form annually or more frequently, as determined by the Compliance Committee. This reinforces the importance of compliance and ensures that employees understand and commit themselves to following the established policies and procedures.

37.2. By implementing these measures, Ashkenazi Trading aims to create a culture of compliance and vigilance among its employees, promoting effective AML/CFT practices and safeguarding against illicit activities.

## 38. Record Keeping

38.1. Ashkenazi Trading recognizes the importance of maintaining comprehensive records related to anti-money laundering and counter-terrorism financing (AML/CFT) efforts. The following documents will be considered as Ashkenazi Trading 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:** Ashkenazi Trading 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:** Ashkenazi Trading 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 the commitment



to educate and update 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:** Ashkenazi Trading 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 Ashkenazi Trading 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. Ashkenazi Trading 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, Ashkenazi Trading aims to demonstrate compliance with regulatory requirements and facilitate effective cooperation with competent authorities in combating money laundering, financing of terrorism and illegal organizations.

## 39. Record Retention Policy

39.1. Ashkenazi Trading 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, Ashkenazi Trading ensures compliance with regulatory requirements and facilitates the availability of relevant information for auditing, monitoring, and investigation purposes.

#### 40. Revision Record

40.1. The Compliance Department of Ashkenazi Trading will securely maintain the master copy of this document, and they will make periodic updates as required. Any revisions made to this document will be recorded and added in the present policy as and when updated. The First policy (V 1.0) was created on [•], in line with AML/CFT Law promulgated by UAE.

### END OF DOCUMENT

VERSION CONTROL	NAME	SIGNATURE
Document Prepared by:	<b>Mr Syed Nadir , Compliance Officer</b> <i>(With support and assistance from Special AML Consultant)</i>	
Document Reviewed and Approved by:	<b>Ms. Gauhar Ashkenazi, Manager</b> <i>(With support and assistance from Special AML Consultant)</i>	





## APPENDIX A – KYC Documents Checklist – Individual

APPENDIX A – NATURAL PERSON (INDIVIDUAL) KYC DOCUMENTS CHECKLIST		
	Document / Information	Completed
1	Basic Customer Information:	
	• Legal name	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Date of Birth	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Place of Birth	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Nationality	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
2	Identity Documents:	
	• Passport	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• National ID	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Visa for the Country of Residence (if applicable)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
3	Address Proof Documents (anyone)	
	• Utility bill (e.g., electricity, water, phone)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Tenancy contract / purchase agreement	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Local authority tax bill	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4	Contact details:	
	• Telephone number(s)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Mobile number (s)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Email address	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5	Verification of contact details above via the due diligence conducted by Ashkenazi Trading staff.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A



6	Ultimate Beneficiary Owner Declaration	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
7	Understanding the source of funds of each Individual / Shareholders / Ultimate Beneficiary Owner / Key Managerial People	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
8	Whether the individual/shareholder/manager is a Politically Exposed Person (PEP) or a Close Associate of a PEP	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
9	In case of salaried person:	
	<ul style="list-style-type: none"> <li>• Proof of Employment</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Proof of Salary</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
10	In case of a businessman:	
	<ul style="list-style-type: none"> <li>• Names and addresses of all businesses, where the customer has a stake above 25%</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• License copy of all businesses</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Main products or services</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Names and addresses of other partners / owners in the businesses</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Main activities geographical areas</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A



## APPENDIX B – KYC Documents Checklist – Corporate

APPENDIX B – LEGAL PERSON (CORPORATE) KYC DOCUMENTS CHECKLIST		
	Document / Information	Completed
1	Proof of legal existence of the Company:	
	• Trade License	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Certificate of Incorporation	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Share Certificates / Shareholders Register	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Memorandum of Association	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Articles of Association	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Tax Registration Certificate	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
2	Proof of the company's Registered Address and Office/Principal Address (primary address where the business activity is performed) in the country of origin and/or physical address within the UAE:	
	• Utility bill (e.g., electricity, water, phone)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Tenancy contract / purchase agreement	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Local authority tax bill	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
3	Contact details:	
	• Office telephone number(s)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Company email address	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Company website	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Key Contact mobile number	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	• Key Contact email address	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
4	Verification of contact details above via the due diligence conducted by Ashkenazi Trading staff.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
5	Ultimate Beneficiary Owner Declaration	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A



6	Board Resolution	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
7	Authorized Traders List (with their specimen signature)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
8	For all Shareholders / Ultimate Beneficiary Owner / Key Managerial People / Authorized Signatories / Powers of Attorney Holders:	
	<ul style="list-style-type: none"> <li>• Passport</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• National ID</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Visa for the Country of Residence (if applicable)</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Address Proof</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
9	Financial Information:	
	<ul style="list-style-type: none"> <li>• Latest Audited Financial Statement (last two years)</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Latest Tax Returns</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
10	Compliance Policies (if available):	
	<ul style="list-style-type: none"> <li>• AML/CFT policies and procedures</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Responsible Supply Chain Policy</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Anti-bribery and Corruption Policy</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Whistleblower Policy</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
11	Details of the company's business including	
	<ul style="list-style-type: none"> <li>• Main products or services</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Names and addresses of parent company and/or subsidiaries, if applicable</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
	<ul style="list-style-type: none"> <li>• Main activities geographical areas</li> </ul>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
12	Understanding the source of funds originating from the Company	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A