EMIRATES MINTING

Anti-Money Laundering, Combating Financing of Terrorism, Non-Proliferation of the Weapons of Mass Destruction, Illegal Organizations, and Sanctions Screening

Policies & Procedures Manual

Document ID: EMF.POL.CP-02

EMIRATES MINTING

Revision History:

No.	Issue No.	Revision No	Revision Date	Drafted / Revised By	Remarks
1	1.0	01	02-06-2025	Compliance Officer	1. Document ID added 2. References section updated. 3. Supply Chain Officer Part added, 4. Employee Screening & Training Part amended
2	1.0	02	20-01-2026	Compliance Officer	Updated with regard to 1. Federal Decree Law (10) of 2025 added & 2. Cabinet Resolution No. (134) of 2025 regarding the Executive Regulations of Federal Decree Law of 2025

Head of Compliance / MLRO	Mr. Malik Umar Mukhtar	Signatures:
Managing Director of the Company	Mr. Mubashar Hussain	Signatures:
CEO of the Company	Mr. Essa Saeed	Signatures:
Effective Date: 20-Jan-2026		

The Management shall approve the initial issue of this Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing and Illegal Organizations, Sanction Screening Policies & Procedures Manual (the "Manual"). All subsequent updates and revisions shall be submitted to the Management for approval.

1. *The latest version of this Manual will be in force. All previous versions of the Manual shall be retained for audit and regulatory reference purposes.*

2. *A soft copy of the Manual shall be available to all relevant employees. One hard copy will be maintained by the Compliance Department.*

3. *Reference shall be made to the definitions provided in the UAE Federal AML legislation, for interpreting any capitalized words not specifically defined herein.*

4. *This Manual is the confidential document of the company. Dissemination of the contents of this Manual to people other than relevant employees of the Company without prior consent of the Management is strictly prohibited.*

5. *Each relevant employee shall provide an undertaking in the format attached in Appendix 1 to this Manual, confirming that he/she has read and understood the contents of this Manual and will abide by the same.*

EMIRATES MINTING

Contents

GLOSSARY

Term	Description
The Company	Emirates Minting Factory L.L.C
DNFBPs	Designated Non-financial Businesses and Professions
MOE	Ministry of Economy
DMCC	Dubai Multi Commodities Center
OECD	Organization for Economic Co-operation and Development
CRM	Customer Relationship Manager
KYC	Know Your Customer
NEO	Accounting system used by the Company
PEP	Politically Exposed Person
EDD	Enhanced Due Diligence
DRC	Democratic Republic of Congo
NRA	UAE National Risk Assessment
AML	Anti-Money Laundering
CFT	Counter Terrorism Financing
TFS	Targeted Financial Sanctions
Sanctions Lists	UN Consolidated and UAE local Terrorist Sanctions Lists
UBO	Ultimate Beneficial Owner
AS	Authorized Signatory
PP	Personal Passport
EID	Emirates ID
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
FIU	Financial Intelligence Unit

EMIRATES MINTING

REFERENCES

1. Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
2. Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
3. Federal Decree Law No. 43 of 2021 on the Commodities Subject to Non-Proliferation
4. Federal Decree Law No. 26 of 2021 to amend certain provisions of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations
5. UAE Federal Decree Law No. 20 of 2018 concerning Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("Federal AML Law")
6. UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences ("Federal CTF Law")
7. 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
8. Cabinet Decision No. 10 of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 concerning Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("Cabinet Decision")
9. Cabinet Decision 74 of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions ("TFS Decision")
10. Cabinet Resolution No. 20 for 2019 concerning the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction and related resolution
11. Resolution No. 11 for 2019 concerning the procedures of implementation the cabinet resolution No. 20 for 2019 concerning the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction and related resolution

12. Cabinet Resolution No. 58 of 2020 on the Regulation of the Procedures of the Real Beneficiary ("UBO Resolution")

13. Cabinet Decision No. (16) of 2021 Regarding the Unified List of the Violations and Administrative Fines for the Said Violations of Measures to Combat Money Laundering and Terrorism Financing that are Subject to the Supervision of the Ministry of Justice and the Ministry of Economy

14. Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organizations Guidelines for Designated Non-Financial Businesses and Professions (DNFBPs), March 2021 ("Guidelines")

15. Ministry of Economy Due Diligence Regulations for Responsible Sourcing of Gold.

16. Supplemental Guidance for Dealers in Precious Metals and Stones. ("DPMS Guidance")

17. Ministry of Economy Implementation Guide for DNFBPs on CUSTOMER DUE DILIGENCE (CDD)

18. Ministry of Economy Implementation Guide for DNFBPs on CUSTOMER RISK-ASSESSMENT (CRA)

19. EOCN Guidance on Proliferation Financing for FIs, DNFBPs, and VASPs.

20. EOCN Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs.

21. EOCN Terrorists and Proliferation Financing Red Flags Guidance.

22. Emirates Bullion Market Committee (EBC) Rules for Risk Based Due Diligence (RBDG) in the gold supply chain.

23. OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas.

24. Ministry of Economy Circulars

25. UAE Federal Law No. 3 of 1987 ("the UAE Penal Code")

(Collectively referred to as "UAE Federal AML legislation")

INTRODUCTION & SCOPE

i. **Emirates Minting Factory L.L.C.**

Emirates Minting Factory L.L.C & Emirates Minting Factory L.L.C (Branch) collectively described as **(The Company)** is a fully integrated innovative precious metals refining and minting service provider with a high-capacity gold refining unit, formed in the Emirate of Dubai, in accordance with the provisions of the Commercial Company Law (Federal Law No. 2 of 2015) came into effect on 1 July 2015 by replacing the previous Law No 8 of 1984 and duly registered under the commercial register at the department of Economic Development with its registered activities Gold & Precious Metal Casting, Gold Refining, Non-Manufactured Precious Metal Trading, including pearls, precious stones, and jewelry trading.

The Company, with its capacity as a responsible gold sourcing and trading company, under the category of Designated Non-Financial Businesses and Professions ("DNFBPs"), declares to abide by the applicable laws, rules & regulations including the standard compliance rules and regulations to Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

This Manual sets out **the Company's** policies and procedures in compliance with applicable provisions of UAE Federal AML legislation.

II. Introduction to AML & the applicable legal framework

Money Laundering is the process by which individuals attempt to conceal the true origin, ownership, and/or use of the proceeds of their criminal activities, thereby avoiding prosecution, conviction, and confiscation of criminal funds. Money laundering can be divided into three stages:

1. **Placement:** The first stage of money laundering is known as 'placement', whereby illicit funds are placed into the legal, financial systems. After getting hold of illegally acquired funds through predicate crimes, criminals move the illicit funds from their source. This is where the illicit funds are 'Washed / Laundered' and disguised by being placed into a legitimate financial system.

2. Layering: The second stage in the money laundering process is referred to as 'layering'. This is a complex web of transactions to move money into the financial system. Once the funds have been placed into the financial system, the criminals make it difficult for authorities to detect laundering activity. They do this by obscuring the audit trail through the strategic layering of financial transactions and fraudulent bookkeeping. Layering is a significantly intricate element of the money laundering process. Its purpose is to create multiple financial transactions to conceal the original source and ownership of the illegal funds.

3. Integration: The third of the stages of money laundering is 'integration'. The illicit funds are now absorbed into the economy. Once the illicit funds have been placed and layered, the funds will be integrated back into the legitimate financial system as 'legal' tender. Integration is done very carefully from legitimate sources to create a plausible explanation for where the Proceeds have come from. These Proceeds are then reunited with the criminal with what appears to be a legitimate source. At this stage, it is very difficult to distinguish between legal and illegal Proceeds.

The Federal AML-CFT-CPF Law defines the criminal offence of Money Laundering as follows:

1. *Anyone who knows, or has sufficient evidence or circumstantial evidence to support his knowledge, that all or some of the funds are derived from a predicate crime and intentionally commits one of the following acts shall be deemed to have committed the crime of money laundering:*

   a. Converts, transfers, or carry out any operation with proceeds with the intent to conceal or disguise their illicit origin.
   b. Conceals or disguises the true nature of the proceeds, their source, location, disposition, movement, ownership, or rights with respect to them.
   c. Acquires, possesses, or uses the proceeds upon receipt.
   d. Helps the perpetrator of the predicate offense to evade punishment.

2. *The crime of money laundering is considered an independent crime and is exempt from the application of the provisions of connection stipulated in Federal Decree-Law No. (31) of 2021 referred to. The punishment or non-punishment of the perpetrator of the original crime does not preclude punishment for the crime of money laundering.*
3. *Conviction for committing the original crime is not required to prove the illicit source of the proceeds, nor is knowledge of the type of original crime from which the proceeds are derived or knowledge of its nature in a specific manner. Knowledge, as an element of the crime, is inferred from the factual and objective circumstances of its commission.*

Money Laundering also includes the closely related subject of Financing of Terrorism & Proliferation; a perpetrator of this crime is described in the Federal CTF Law as:

1. *Anyone who intentionally provides, collects, or makes available funds by any means, directly or indirectly, including the use of digital systems, virtual assets, or encryption technologies, knowing that they will be used, in whole or in part, in any of the following cases, shall be considered to have committed the crime of financing terrorism:*
   a. Committing a terrorist act or terrorist acts.
   b. By a terrorist or terrorist organization.
   c. Financing the travel of individuals to a country other than the one in which they reside or hold citizenship, for the purpose of committing, preparing, planning, participating in, or facilitating a terrorist act, or providing the necessary funding for training for a terrorist act or receiving such training.
2. *For the purposes of Clause (1) of this Article, funds used in the crime of financing terrorism include any funds used, in whole or in part, whether from a legitimate or illegitimate source, regardless of whether they are actually used to commit or attempt to commit a terrorist act or are linked to any specific terrorist act. The crime of financing terrorism is committed regardless of whether the person accused of committing it is present in the country in which the terrorist or terrorist organization is located, in the country in which the terrorist act was or will be committed, or in another country.*

3. *In circumstances other than those permitted or authorized in accordance with the legislation in force in the country and the provisions of treaties or agreements to which the country is a party, anyone who intentionally commits any of the following shall be deemed to have committed the crime of financing the proliferation of arms:*
   a. *Provides, collects, or makes available funds by any means, directly or indirectly, knowing that they will be used, in whole or in part, to manufacture, acquire, possess, develop, produce, sell, supply, export, transship, broker, transport, transfer, stockpile, or use weapons of mass destruction, their means of delivery, and related materials, including dual-use technologies and goods if used for such a purpose.*
   b. *Any other act in accordance with resolutions adopted by the United Nations Security Council under Chapter VII of the Charter of the United Nations on the prevention, suppression, and suppression of the proliferation of weapons and its financing.*

4. *Knowledge, as a component of the crime of financing terrorism and the crime of financing arms proliferation, is derived from the factual and objective circumstances of their commission.*

Non-Proliferation is defined as "Preventing the illegal and unauthorized trading of goods that contribute to the production or development of weapons of mass destruction, associated technology and means of delivery."

Weapons of Mass Destruction are defined as Weapons that can cause harm to numerous human beings and cause threats to life and biosphere through their catastrophic consequences, such as nuclear, biological, chemical and radiological weapons.
The crime of Financing of Illegal Organizations, i.e. "*Any physical or legal action aiming at providing funding to an illegal organization*" (an organization whose establishment is criminalized, or which pursue a criminalized activity), "*or any of its activities or members*".

In addition, **the Company**'s AML/CFT/CPF policies and procedures must also ensure that sanctions list issued by the UAE Government, as well as the United Nations Security Council, are screened against; any associated instructions on prohibited transactions, asset freezing, etc., must also be complied with in accordance with TFS Decision.

In this regard, it is important for all Employees of **the Company** to familiarize themselves with what may constitute a crime of Money Laundering, Terrorists Financing, and Proliferation Financing (ML/TF/PF) and the procedures to be adhered to prevent this crime from taking place within **the Company**. Overall responsibility for ensuring compliance with the Federal AML/CFT/CPF legislation rests with the senior management of **the Company**. In carrying out their responsibilities under this module every member of the senior management must exercise due skill, care, and diligence.

Ministry of Economy, UAE may act against any of the following people for any breach of the provisions of the applicable AML-CFT-CPF laws, regulations, and/or guidance:
- the Company
- any member of the senior management; or

• any Employee of **the Company**.

1. POLICY OBJECTIVES

It is the policy and practice of the Company to maintain high standards of ethical conduct, to comply with all applicable laws, and to do business only with people who themselves abide by law and ethical principles. The Company is committed to comply with all applicable laws and regulations relating to Anti-Money Laundering, Counter-Terrorism Financing, Counter Proliferation Financing and Sanctions Compliance.

The objectives of **the Company**'s AML-CFT-CPF policies are:

- To provide a framework to detect and minimize the risks involving Money Laundering and Terrorist & Proliferation Financing activities.
- To comply with the U.A.E.'s AML/CFT/CPF laws and regulations.
- To enable all its Employees to detect suspicious customers or transactions, and minimize the risk of the Company being used, directly or indirectly by money launderers and/or terrorists for terrorism & proliferation financing activities.

All employees of the Company, including part-time employees and outsourced service providers, are required to read this Manual thoroughly, assimilate its contents, and ensure its implementation in letter and spirit.

2. ADMINISTRATION STRUCTURE

The Company has implemented an administration structure comprising - (a) the Management, (b) Compliance Officer and (c) Internal Audit. Significant responsibilities have been apportioned in line with corporate governance and regulatory requirements to ensure adequate oversight and monitoring of AML-CFT-CPF systems and controls.

The Management

As per the Company Resolution dated 10th Jan 2024, The Senior Management of Emirates Minting Factory LLC is consisting of the Managing Director and the Head of Finance of the company as approved by the Chairman / Sole Shareholder of the Company. The Management takes the ultimate responsibility of laying down a top-to-bottom compliance culture and provides adequate oversight on the AML-CFT-CPF processes. The Management takes the overall responsibility of managing the risks relating to AML-CFT-CPF and The Management will-

- provide strategic direction.
- set the risk management policy; and
- decide the nature and extent of risks acceptable.

The Management will also be responsible for all day-to-day operations, will ensure that the policies, procedures, and controls laid down by the Compliance Officer are well-communicated and incorporated into the day-to-day operations.

Compliance Officer

The Compliance Officer (CO) shall be appointed by the Management. **The Company** shall ensure that the CO is able to operate and functions independently from other departments and individuals within the organization structure and is provided with unfettered access to the Management. He/she shall be a senior member of staff and shall have the necessary competence, knowledge, experience, and training in AML/CFT/CPF Compliance and KYC processes, shall be provided with all resources necessary to perform the function and role in accordance with the UAE AML-CFT-CPF Laws and Rules, and shall be able to communicate critical information to the management, staff, and customers. The CO's tasks can be grouped broadly into the following three categories- (a) AML/CFT/TFS Reporting, (b) AML/CFT/CPF/TFS and Responsible Sourcing Program management and (c) AML/CFT/CPF/TFS and Responsible Sourcing Training and Development. The Compliance Officer shall carry out the following tasks in a fully independent manner:

a) Identifying cases of money laundering, financing of terrorism & proliferation and illegal organizations.
b) Reviewing records and receiving, examining, and investigating suspicious transactions and taking a decision to notify or close them, and providing reasons confidentially.
c) Providing semi-annual reports (once in six months) to the senior management (refer to Procedure CP-19 Management Reporting). The report shall cover Compliance Officer review of rules and procedures related to combating money laundering and the financing of terrorism & proliferation and illegal organizations, providing suggestions to upgrade and develop them, and submitting copies of such reports along with the senior management comments and decisions to the Ministry of Economy (MOE).
d) Developing and implementing training programs and plans for employees; and
e) Cooperating with the Ministry of Economy and FIU in providing information and documents requested by them from time to time.

The CO's Functions and Duties, in addition to those identified above, include:

(a) submitting any Suspicious Transaction or Activity Report (STR/SAR) to the FIU through online portal GoAML; and
(b) submitting a copy of each semi-annual report (together with any notes and resolution of the senior management in response to such report) to MOE.
(c) reviewing and signing off on each KYC/CDD & supply chain due diligence exercise.
(d) continually monitoring and assessing **the Company**'s AML/CFT/CPF & supply chain due diligence processes.
(e) ensuring that the Company's AML/CFT/CPF & supply chain policies and procedures, and each associated due diligence exercise carried out by **the Company**, are adequate to be compliant with the UAE AML-CFT-CPF Law.

(f) training staff and promoting awareness within **the Company** with respect to AML/CFT/CPF & responsible supply chain due diligence, **the Company**'s AML/CFT/CPF & supply chain policies and procedures, KYC requirements, and applicable laws; and
(g) updating **the Company**'s AML/CFT/CPF & supply chain policies and procedures, and related processes, as and when required.

Supply Chain Officer

The Supply Chain Officer shall be a senior member of staff and shall have the necessary competence, knowledge, experience, and training in Supply Chain Due Diligence and KYC processes, shall be provided with all resources necessary to perform the function and role in accordance with the MOE Due Diligence Regulations for Responsible Sourcing of Gold and EBC Rules for RBDG , and shall be able to communicate critical information to the management, staff, and Suppliers. The Supply Chain Officer shall carry out the following tasks in a fully independent manner:

(a) review and sign off on each gold supply chain due diligence exercise.
(b) continually monitor and assess the company's supply chain due diligence processes.
(c) ensure that the Policy and each associated due diligence exercise carried out by the company are adequate for the purposes of these Rules for RBDG & MOE Due Diligence Regulations.
(d) train staff and promote awareness within the organization with respect to responsible supply chain due diligence, the company's Policy, KYC requirements and applicable laws; and
(e) update the Policy and related processes as and when required.

Internal Audit

The role of internal audit is to verify whether the risk control functions and processes are effective and provide observations to the Management and Compliance Officer. Such independent evaluation on a regular basis will enrich the control framework.

3. MAIN ELEMENTS OF CDD PROCESSES

In order to meet the minimum Customer Due Diligence requirements as laid out in the Cabinet Decision, the following information shall be collected and maintained to verify the identity of the customer and the UBO of the customer before or during the establishment of the business relationship or opening of the customer's account, or before executing a transaction for a customer with whom there is no business relationship, and shall also be updated on an ongoing basis:

i. For each UBO of customer that is a natural person:
    1. Full name (as shown on an identification card or travel document)
    2. Nationality
    3. Residency

4. Address
5. Place of birth (as shown in an identification card or travel document)
6. Employer details (if any), and
7. A copy of the original and valid identification card or travel document
8. Contact Details

ii. For each customer or UBO of a customer that is a corporate entity:

1. Legal status and category of entity
2. Full name
3. Memorandum of Association
4. Information on the intended purpose and nature of the business relationship
5. Information on the customer's business activities as well as their ownership and control structure
6. Articles of Association, or any similar documents, attested by the competent authority within the UAE
7. Address of its registered office and principal place of business (if different)
8. Names of the relevant persons holding senior management positions
9. KYC documents as required in (i) or (ii) for each legally authorized representative
10. Copy of the instrument(s) authorizing each of its legally authorized representatives
11. KYC documents required (as in (i) for natural persons and as in (ii) for corporate entities) for each UBO with an ownership interest of 25% or more, except for publicly listed companies, or their subsidiaries, for which such information is publicly available; where no such controlling ownership interest can be identified, the natural person(s) holding the position of senior management officer(s) shall be considered the UBO(s) and their identity shall be verified as stipulated in (i)
12. Copy of its constitutional documents, and
13. Copy of its valid commercial or professional license or registration
14. If the customer is a Legal Arrangement, verification of the identity of the settler, trustee(s), or any person holding similar positions, beneficiaries or class of beneficiaries, and the natural person(s) identified as UBO(s)

4. CUSTOMER RISK ASSESSMENT

i. Customer Due Diligence

a) **The Company** will have agreements in place with customers that support responsible sourcing of minerals from high risk and conflict-affected areas in order to avoid any action, which may contribute to the financing of conflict.

b) **The Company** will be using intelligence systems such as World Check to scan customers' background against sanction lists including UAE, UN, EU, OFAC, and HM Treasury lists.

c) **The Company** will not open any account or conduct any business transactions with a potential client unless the customer due diligence (CDD), including the Know Your Customer (KYC) process, procedure is implemented, and relevant forms are completed and approved by the compliance department. This process is described in the Customer Account Opening Procedure (CP-01).

d) The KYC/CDD review, and screening process must be conducted at least once a year for all Low-Risk customers. Higher risk customers undergo the KYC/CDD review, and screening process more frequently as per the Risk Assessment Procedure (CP-02) and the Enhanced Due Diligence (EDD) Procedure (CP-03).

e) **The Company** does not accept any walk-in customers' transactions. All new customers are subject to the KYC/CDD process, and no transactions will be processed until the full process is completed and approved by the Compliance Department.

f) Customer information needs to be updated on regular basis as per the Updating KYC Records Procedure (CP-05). **The Company** will not continue any business relationship with customers who fail to update their information when requested to do so.

g) **The Company** should determine the source of precious metal for all its supply chain to make sure that it is compliant with the related regulations for responsible sourcing.

h) Customer accounts which do not have transactions for 3 months will be blocked and marked as inactive.

i) It is strictly prohibited to open accounts with assumed names, and the Company will rely on the account holder names as in passport or trade license in case of juridical persons.

ii. Risk Assessment

The Company will use a risk assessment matrix to assess the risk rating of its customers, which will be used to define the degree of Due Diligence to be executed for certain customers. This is done through the Risk Assessment procedure (CP-02). The following actions will be taken once a Risk Rating has been assigned to a customer:

Low Risk – Start or continue trading activities.

Medium Risk – Start or continue trading activities with ongoing monitoring of transactions, KYC/CDD review, and screening process as per the Risk Assessment Procedure (CP-02).

High Risk – Suspend trading activities while initiating Enhanced Due Diligence (CP-03) by obtaining additional information / data confirming or refuting the adverse risk assessments or disengage from the source(s) of the risk within a reasonable time frame (to be assessed on a case-by-case basis).

Where a High-Risk rating has been assessed for any customer, it shall immediately be escalated for review and approval of Senior Management.

The Company keeps a list of the countries to be tagged as High Risk or Unacceptable Supply Source that considers the NAMLCFTC / Financial Action Task Force (FATF) list of jurisdictions, as either High-Risk and Non-Cooperative Jurisdictions, or Jurisdictions with Strategic AML Deficiencies under Increased Monitoring as well as other factors. Customers from these countries are subject to the Enhanced Due Diligence Procedure.

In addition, any transactions involving from an individual or entity hailing from (by virtue of nationality, residency, place of incorporation) a country classified as a 'high-risk jurisdiction subject to a call for action' by FATF, shall be reported to the FIU before conducting such a transaction. **Such reported transactions may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.**

Our risk assessment will extend to our customers' supply chain, i.e., their customers / Suppliers.

iii. Cash, checks, and transfers

a) **The Company** does not accept any cash payment from any customer unless their amounts are less than UAE Dirhams (AED) 55,000 and only for the following purposes:

- Paying off visa charges.
- Settlements related to the closing of accounts.
- Refining charges.
- Assaying charges.
- Other trade-related expenses incurred by customers, government fees and related charges

As per the UAE Precious Metals Business practice **the company** could pay in Cash to the customer upon request and providing the valid and acceptable reason for demanding payment in cash.

In the event of any cash transactions related to precious metal receipt/payment with individuals (resident or non-resident) equal to or exceeding AED 55,000, the following additional procedures shall be followed:

- Obtain identification documents (Emirates ID or Passport) and register the information in the Financial Intelligence Unit's ("FIU") GoAML platform using the 'Dealers in Precious Metals and Stones Report' (DPMSR).

In the event of any cash transactions or wire transfers related to precious metal receipt/payment with companies/legal entities equal to or exceeding AED 55,000, the following additional procedures shall be followed:

- Obtain a copy of the trade license, and identification documents (Emirates ID or passport) of the person representing the company and register the information in the Financial Intelligence Unit's ("FIU") GoAML platform using the 'Dealers in Precious Metals and Stones Report' (DPMSR).

b) It is the policy of **the Company** not to accept cheques issued by foreign banks.

c) It is not advisable to accept cheques issued by money exchanges on behalf of customers. However, in case wire transfers are not possible from certain countries, or it might take extended period, cheques from money exchanges can be accepted only if the Enhanced Due Diligence Procedure (CP-03) was implemented to ensure a clean source of the funds handed to the money exchange branch in the country of origin.

d) All payments from out-of-the-country clients must happen through wire transfers. Cheques are only accepted by customers within the UAE. Details for responsible payments are given in the related payments and transaction compliance procedures.

e) Internal transfers of funds or gold balances between **the Company's** customer accounts are not allowed unless it is related to gold movement transaction. This is implemented through the guidelines provided in the Internal Transfers Compliance Procedure (CP-12).

f) No 3rd party transfers allowed on behalf of the customers. Payments towards customers must happen through wire transfers initiated by the same customer, or from a related customer of **the Company**.

g) Payments to customers are only made to their own bank accounts in the country of origin. Any requests for transfers otherwise should be authorized by the Management and Compliance Department after implementing the Enhanced Due Diligence Procedure.

h) Payees of cheques should be the customer company name itself as per the Company system. No cheques are allowed to be paid to any other beneficiaries, including owners and employees of the customer. Any request from the customer to issue a cheque to any other beneficiaries shall be rejected and reported to the Management and Compliance Department.

5. POLITICALLY EXPOSED PERSONS (PEPs)

The Cabinet Decision defines PEPs as:
"Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organization or any prominent function within such an organization; and the definition also includes the following:

1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents).

2. Associates known to be close to the PEP, which include:
(a) Individuals have joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP.
(b) Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

Where the due diligence process identifies the customer or any of its UBOs as a foreign PEP, the matter shall be immediately notified to the Management for their approval for **the Company** to continue to engage business with the concerned customer. In addition, **the Company** shall establish the source of wealth of the relevant PEP, and people associated with them, and implement an adequate enhanced transaction monitoring system for any transactions to be entered into with the relevant PEP.

Where the due diligence process identifies the customer or any of its UBOs as domestic PEPs or individuals previously entrusted with prominent functions at international organizations, **the Company** shall take sufficient measures to identify whether the customer or its UBOs meet these definitions and shall take all the additional measures required for foreign PEPs where the relevant customer relationship is High Risk.

6. REPORTING SUSPICIOUS ACTIVITY / TRANSACTIONS

It is the endeavor of **the Company** to have in place appropriate systems and controls that monitor, detect and report suspicious activity or transactions. The onus is on all employees of **the Company**, both internal and outsourced (full-time and part-time) to detect, report and prevent such transactions from taking place. Thus, **the Company** has adopted the policy as described below that relates to identifying transactions of a suspicious nature and immediately reporting the same to the Compliance Officer, who shall take further action as required.

i. Suspicious Activity/Transactions

A suspicious transaction refers to any transaction, attempted transaction, or funds which the Company has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing—any of the following:

- The proceeds of crime (whether designated as a misdemeanor or felony, and whether committed within the State or in another country in which it is also a crime).
- Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organizations; or
- Being intended to be used in an activity related to such crimes.

Identification of suspicious activity/transaction differs from case to case. The general rule is that any activity/transaction that appears to deviate from normal and known course of conducting business needs to be carefully examined by the employee, who shall have to be completely satisfied that no foul play is involved. Circumstances that might give rise to suspicion or reasonable grounds for suspicion include:

- Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection.

- Transactions requested by a person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of the Firm in relation to a particular customer.

- Where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection.

• Where a customer's refusal to provide the information requested without reasonable explanation.

• Where a customer who has just entered a business relationship uses the relationship for a single transaction or for only a very short period.

• Extensive use of offshore accounts, companies, or structures in circumstances where the customer's economic needs do not support such requirements.

• Unnecessary routing of funds through third party accounts; or

• Unusual transactions without an apparently profitable motive.

A list of red-flag indicators of potentially suspicious transactions is provided in Appendix- 3. The presence of any of these red flags is an indication that enhanced due diligence, or further investigation may be required, so that appropriate determination can be made by the Compliance Officer as to whether the transaction is suspicious or not.

Employees must also ensure that they do not disclose, directly or indirectly, to the customer or any other person(s) that a SAR/STR has been, or is about to be, filed, and neither should they disclose any information or data contained within the SAR/STR, nor that an investigation is being conducted in relation to the SAR/STR.

ii. Internal Reporting

Whenever any Employee of the Firm, acting in the ordinary course of his employment, either:

- knows.
- suspects; or
- has reasonable grounds for knowing or suspecting.

that a transaction, attempted transaction, or other customer-related funds constitute proceeds or crime or are related to the crimes of Money Laundering or Financing of Terrorism & Proliferation or Financing of Illegal Organizations, Employee must promptly notify the Compliance Officer and provide the Compliance Officer with all relevant details. The format for the Employees to make an Internal Suspicious Activity Report (Internal SAR), containing the minimum required information for the Compliance Officer to take further action.

iii. External Reporting

Once an Internal SAR is received:

a. The Compliance Officer shall verify the information provided, conduct necessary investigations to conclude whether an External SAR needs to be filed with the FIU through online portal GoAML.

b. Investigations by the Compliance Officer may include interviewing the employee who filed the report, gathering relevant data, verifying the documents produced, and discussing with the management.

c. If it is decided that no further action needs to be taken, the Compliance Officer shall record his reasons for such a finding and report the same to the Management.

d. If it is decided that an External SAR needs to be filed with the FIU, then the SAR has to be submitted through online portal GoAML, and a copy of the report must also be provided to MOE

It is to be noted that failure to report suspicions of money laundering or terrorist & proliferation financing may constitute a criminal offence that is punishable under the laws of the UAE.

The Firm will not prejudice an Employee who discloses any information regarding money laundering or terrorist & proliferation financing to MOE - FIU or to any other relevant body involved in the prevention of money laundering or terrorist & proliferation financing.

iv. Timelines for SAR/STR

SAR/STRs are required to be reported to the FIU without any delay. Therefore, relevant Employee shall provide Internal Reporting directly to the Compliance Officer **immediately** once the customer behavior or suspicious nature of the transaction has any one of the indicators listed in Appendix-3. The Compliance Officer shall quickly review the Internal SAR report to determine whether further internal investigation (if any) is required before suspicion or reasonable grounds for suspicion are established. The Compliance Officer shall commence further investigation as may be required immediately and ensure the completion of such investigation on a priority basis. The Compliance Officer shall promptly submit SAR through GoAML portal, soon after suspicion or reasonable grounds for suspicion is established.

It is the policy of **The Company** to submit SAR/STR to FIU without any delay. The Compliance Officer shall record and monitor the timelines and delays in internal reporting or further investigation shall be reported to the management. Any delay by the relevant Employee will result in disciplinary action by the management.

Strict confidentiality shall be maintained regarding the internal SAR/STR reporting, further investigation, or SAR/STR reporting to FIU.

Management, employees, and authorized representatives are protected by the UAE Federal AML/CFT/CPF legislation from any administrative, civil, or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU.

7. MONITORING AND SURVEILLANCE

All client documentation and records relating to AML/CFT/CPF processes shall be maintained, continually monitored, and periodically updated in line with the Cabinet Decision requirements. In addition, all

AML/CFT/CPF systems and controls should also be regularly reviewed and updated where necessary, to ensure full compliance with all applicable laws, regulations, and international standards.

The Company shall also ensure that its internal documentation and records cover internal inventory and transactional documentation, including among others:

(a) details of physical form, type (i.e., Mined Gold, or Recycled Gold), and physical description of gold, including any imprints and/or hallmarks.

(b) Full KYC due diligence of all customers including their due diligence practices e.g., information on customers' due diligence process and KYC requirements.

(c) The dates of applicable purchases and sales include financial transaction information (such as payment amount, currency, mode of payment, etc.).

(d) the mode of payment.

(e) a "Track and Trace" mechanism for tracing products back to purchased material, which shall include (where applicable):

i. shipping/transportation documents.
ii. sales documents with specific lot number.
iii. mining license(s) and related permission (for mined gold).
iv. import/export license(s) and form(s); and
v. Reconciliation of documentation.

8. SANCTIONS COMPLIANCE

The Company shall comply with all targeted sanctions imposed by the UNSC and UAE by adopting the following additional due diligence and monitoring procedures-

- Subscribe for the United Nations Consolidated and UAE local Terrorist sanctions lists through https://www.uaeiec.gov.ae/en-us/un-page to receive the automatic notifications of any change in said lists through email.
- Prepare / download the list of natural persons or legal entities designated by UNSC and UAE Cabinet by obtaining information from https://www.uaeiec.gov.ae/en-us/un-page , update these lists as and when there are any addition or removal in said lists notified by relevant authority through email.
- Conduct screening on new, existing, and potential customers, prior to every transaction including, without limitation, the following:
  - Purchaser & seller
  - Shipper and freight forwarder

- Source of funds whether derived from any asset owned or controlled by a designated person

- With regards to Circular No. 5/2021 issued by Ministry of Economy dated 25/08/2021, The Company has the obligation to report any match found during screening through below mentioned two TFS related reports using GoAML platform-

  - Confirmed Name Match Report (CNMR) formally known as Funds Freeze Report (FFR).
  - Partial Name Match Report (PNMR).

- If a confirmed match is found then-

  - Implement all necessary measures without delay as outlined in the Cabinet Decision (74) of 2020, Guidance on Targeted Financial Sanctions issued by the EO-IEC.
  - Report any freezing measure, prohibition to provide funds or services, and any attempted transactions to the Ministry of Economy and the Executive Office – IEC via the GoAML platform within two business days by selecting the Confirmed Name Match Report (CNMR).
  - Ensure all the necessary information and documents regarding the 'confirmed match' are submitted along with the CNMR.
  - Uphold freezing measures related to the 'confirmed match' until further instructions are received from Executive Office – IEC.

Notify and share a copy of the report with Ministry of Economy through this email: sanctions@economy.ae

- If a potential match is found then-

  - Suspend without delay any transaction and refrain from offering any funds or services.
  - Report the 'potential match' to the Ministry of Economy and the Executive Office – IEC via the GoAML platform by selecting the Partial Name Match Report (PNMR).
  - Ensure all the necessary information and documents related to the potential match are 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.
  - Notify and share a copy of the report with Ministry of Economy through this email sanctions@economy.ae

9. EMPLOYEES SCREENING

The Company shall collect details such as - employee's full name, date and place of birth, nationality, residence, contact details, previous activities and occupations, copy of identity document carry out background reference checks of the candidates and screen them using World-check at least every twelve months as per EBC RBDG

Rules. Candidates found suitable without any criminal history shall only be considered for appointments in accordance with the Company's HR Policy.

10. RECORD-KEEPING

The Company shall retain all relevant files, records, documents, communications, and forms for a minimum period of **5 years** from the date of –

a) most recent transaction relating to the latest intake of material from a customer.
b) Conclusion of the latest complete inspection by the DMCC or the Ministry of Economy.
c) closing of the account of a customer.
d) termination of relationship of a customer; and
e) closing of investigation on a particular transaction or customer.

The Company shall retain all relevant files, records, documents, communications, and forms relating to relations that were not entered into or progressed with a potential customer for a minimum period of 5 (five)**years**.

11. CONTRAVENTIONS AND PENALTIES

Non-compliance with this Policy and any applicable laws and regulations by the employees may result in the Company, as well as the relevant employees, facing criminal liability for the offence of money laundering as per the Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing and the Federal Law by Decree No. (31) of 2021 Promulgating the Crimes and Penalties Law, as well as regulatory enforcement action by the Ministry of Economy ("MOE"). The punishments for individuals found guilty under the UAE AML Law include, without limitation, the following-

Article	Offence	Punishment
26 (1)	Whoever commits a money laundering crime shall be punished by	Imprisonment for a period of not less than (1) one year and not more than (10) ten years and a fine of not less than (100,000) one hundred thousand dirhams and not more than (5,000,000) five million dirhams or the equivalent of the value of the relevant criminal property, whichever is greater.

26(2)	If the perpetrator commits a money laundering crime in any of the following cases: A. Exploiting his influence or authority granted to him by virtue of his job or professional activity. B. Through a non-profit organization. C. Through an organized criminal group. D. If the original crime is one of the crimes mentioned in Chapter Seven of Part One and Chapter One of Part Two of Book Two of Federal Decree-Law No. (31) of 2021 referred to, or one of the crimes mentioned in Federal Decree-Law No. (30) of 2021 referred to. E. Recidivism.	Temporary imprisonment and a fine of not less than (1,000,000) one million dirhams and not more than (10,000,000) ten million dirhams or the equivalent of twice the value of the relevant criminal property, whichever is greater,
26(3)	Whoever commits a crime of financing terrorism shall be punished by	Life imprisonment or temporary imprisonment for a period of not less than (10) ten years and a fine of not less than (1,000,000) one million dirhams and not more than (10,000,000) ten million dirhams or the equivalent of twice the value of the relevant criminal property, whichever is greater.
26(4)	Whoever commits a crime of financing the proliferation of arms shall be punished by	Temporary imprisonment and a fine of not less than (1,000,000) one million dirhams and not more than (10,000,000) ten million dirhams or the equivalent of twice the value of the relevant criminal property, whichever is greater.
26(5)	Whoever attempts to commit money laundering, terrorism financing, or proliferation financing crimes shall be punished by the penalty prescribed for the full crime.	
26(6)	The court, upon the request of the Public Prosecutor or his delegate, or on its own initiative, may reduce or exempt from the penalty stipulated in this article any of the perpetrators who takes the initiative and provides the judicial or administrative authorities with information related to any of the crimes punishable in this article, provided that this leads to the disclosure of the crime or its perpetrators and proving them against them, or the arrest of one of them, or the seizure of criminal property.	
27(1)	Any legal person whose representatives, managers or agents, for or in its name, commit money	A fine of not less than (5,000,000) five million dirhams and not more than (100,000,000) one hundred million dirhams,

	laundering, terrorism financing or arms proliferation financing crimes shall be punished by	or the equivalent of the value of the relevant criminal property, whichever is greater.
27(2)	Any legal person whose representatives, managers or agents, for or in its name, commit any of the following crimes: a. Failure to report SAR/STR b. Tipping off, notifies or alerts a person or discloses transactions under review regarding any information related to suspicious transactions or that the competent authorities are investigating. c. Whoever possesses, conceals, or conducts any transaction involving funds where there is sufficient evidence or circumstantial evidence of the illegality of its source or concealment of its true beneficiary d. engage in any financial activity, specified non-financial business or profession, or virtual asset service provider activity without a license, registration, or authorization from the competent authority or regulatory authorities. e. Anyone who violates the instructions of the Executive Office or other competent authorities related to the targeted financial penalties f. Anyone who refrains from providing additional information when requested, or intentionally conceals information that must be disclosed, or intentionally provides incorrect information. g. Whoever intentionally provides incorrect or misleading information regarding the beneficial owner to any authority competent to request such information, to financial institutions, designated non-	A fine of not less than (200,000) two hundred thousand dirhams and not more than (10,000,000) ten million dirhams.

	financial businesses and professions, or virtual asset service providers h. Whoever unlawfully enables a third party to benefit from his account with financial institutions or virtual asset service providers i. Failure to Identify, understand, and manage crime risks in its field of work, assess, document, and update them on an ongoing basis, taking into account the risk-based approach, maintain, or provide any services to accounts or conduct any financial or commercial transactions under an anonymous, fictitious, pseudonymous, or numbered name, Establishing internal policies, controls, and procedures approved by senior management to enable it to manage and mitigate identified risks, and to continuously review and update them, and to apply them to all its branches and subsidiaries in which it holds a majority stake. shall be punished by	
27(3)	In the event that a legal person is convicted of a crime of terrorism financing or a crime of arms proliferation financing, the court shall order its dissolution and the closure of the headquarters where it carries out its activity.	
27(4)	In the event that a legal person is convicted of a money laundering crime, or in the event of failure to declare when bringing into or taking out of the country currencies, negotiable bearer financial instruments, precious metals, or valuable stones, in accordance with the disclosure system issued by the Federal Authority for Identity and Citizenship, Customs and Ports Security in coordination with the Central Bank, the court may order	Dissolution and the closure of the headquarters where it carries out its activity.

27(5)	In cases where any of the crimes stipulated in Clauses (1) and (2) of Article 27 are committed, the person responsible for the actual management of the legal person shall be	Punished with imprisonment and a fine, or with one of these two penalties, if it is proven that he knew about them and they occurred due to his breach of his job duties.
27(6)	When issuing a conviction, the court may order the publication of a summary of the judgment by appropriate means, at the expense of the convicted person.	
28	Anyone who intentionally or through gross negligence fails to report if suspect or have reasonable grounds to suspect a transaction or funds that are, in whole or in part, proceeds of a crime, or are suspected of being related to or intended to be used in a crime, regardless of their value, shall be punished by	Imprisonment and a fine of no less than (100,000) one hundred thousand dirhams and no more than (1,000,000) one million dirhams, or by one of these two penalties.
29(1)	Whoever notifies or alerts a person or discloses transactions under review regarding any information related to suspicious transactions or that the competent authorities are investigating or investigating them shall be punished by	Imprisonment and a fine of not less than (50,000) fifty thousand dirhams, or by either of these two penalties.
29(2)	Whoever intentionally or through gross negligence fails to perform the duties of managing the funds assigned to him, or by any order issued by a competent authority to seize, freeze, or otherwise take precautionary measures, shall be punished by	Imprisonment and a fine of not less than (50,000) fifty thousand dirhams, or by either of these two penalties.
29(3)	if any of the acts mentioned in Clauses (1) and (2) of this Article result in the inability to seize the proceeds, their destruction, or the loss of their value the penalty shall be	Imprisonment for a period of not less than one year and a fine equal to the value of the proceeds, but not less than (100,000) one hundred thousand dirhams
30(1)	Whoever possesses, conceals, or conducts any transaction involving funds where there is sufficient evidence or circumstantial evidence of the illegality of its source or concealment of its true beneficiary shall be punished by	Imprisonment for a period of no less than (3) three months and a fine of no less than (50,000) fifty thousand dirhams, or by either of these two penalties.
30(2)	Whoever promotes, offers for sale, provides services, or deals in virtual assets characterized by complete anonymity, or prevents or hinders the ability of the competent authorities to track the	imprisonment for a period of no less than (3) three months and a fine of no less than

	transaction and its parties, or any type of unlicensed accounts or technologies that allow this, shall be punished by	(50,000) fifty thousand dirhams, or by either of these two penalties.
32	Engagement on natural or legal person in any financial activity, specified non-financial business or profession, or virtual asset service provider activity without a license, registration, or authorization from the competent authority or regulatory authorities, shall be punished by	Imprisonment and a fine of no less than (200,000) two hundred thousand dirhams and no more than (10,000,000) ten million dirhams, or by one of these two penalties.
33	Anyone who violates the instructions of the Executive Office or other competent authorities related to the targeted financial penalties shall be punished by	Imprisonment and a fine of not less than (20,000) twenty thousand dirhams, or by one of these two penalties.
34	Any person fails declare when bringing into or taking out of the country currencies, negotiable bearer financial instruments, precious metals, or valuable stones, in accordance with the disclosure system issued by the Federal Authority for Identity and Citizenship, Customs and Ports Security in coordination with the Central Bank or refrains from providing additional information when requested, or intentionally conceals information that must be disclosed, or intentionally provides incorrect information, shall be punished by	Imprisonment and a fine, or by one of these two penalties. The court may, upon conviction, order the confiscation of the seized funds without prejudice to the rights of third parties acting in good faith.
35(1)	Whoever intentionally provides incorrect or misleading information regarding the beneficial owner to any authority competent to request such information, to financial institutions, designated non-financial businesses and professions, or virtual asset service providers shall be punished by	Imprisonment and a fine of no less than (20,000) twenty thousand dirhams, or by either of these two penalties.
35(2)	Whoever unlawfully enables a third party to benefit from his account with financial institutions or virtual asset service providers, if there is sufficient evidence or indication of his knowledge, that the purpose of this is to misuse the account. shall be punished by	imprisonment and a fine, or by either of these two penalties,

35(3)	Failure to Identify, understand, and manage crime risks in its field of work, assess, document, and update them on an ongoing basis, taking into account the risk-based approach and the multiple aspects of risk defined by the executive regulations. open, maintain, or provide any services to accounts or conduct any financial or commercial transactions under an anonymous, fictitious, pseudonymous, or numbered name. Failure to establish internal policies, controls, and procedures approved by senior management to enable it to manage and mitigate identified risks, and to continuously review and update them, and to apply them to all its branches and subsidiaries in which it holds a majority stake.	Imprisonment and a fine of no less than (10,000) ten thousand dirhams, or by either of these two penalties.
36(1)	If a foreigner is sentenced to a custodial penalty for a money laundering crime or one of the felonies stipulated in the Decree-Law	Shall be deported from the country
	Without prejudice to the provisions of Clause (1) of this Article, if a foreigner is sentenced to a custodial penalty in other misdemeanor cases stipulated in the Decree-Law	Court may order his deportation from the country, or order deportation instead of sentencing him to a custodial penalty.
37(1)	As a result of providing any requested information or violating any restriction imposed by a legislative, contractual, or administrative provision to ensure the confidentiality of information, even if they did not know precisely the nature of the crime or its actual occurrence, unless it is proven that the reporting was made in bad faith with the intent to harm others.	No criminal, civil, or administrative liability shall be incurred by regulatory authorities, the Unit, law enforcement agencies, financial institutions, designated non-financial businesses and professions, virtual asset service providers, board members, employees, and legally authorized representatives,

In addition, Article 17 of the Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, empowers the Supervisory authority to impose the following administrative penalties on the financial institutions, designated non-financial businesses

and professions, virtual asset service providers, and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning
b) An administrative fine of not less than (10,000) ten thousand dirhams and not more than (5,000,000) five million dirhams for each violation.
c) Preventing the violator from working in the sector related to the violation for a period determined by the regulatory authority.
d) Restricting the powers of members of the board of directors, members of the executive or supervisory management, managers, or owners proven responsible for the violation, including appointing a temporary auditor.
e) Suspending managers, members of the board of directors, members of the executive or supervisory management proven responsible for the violation for a period determined by the regulatory authority or requesting their replacement.
f) Suspending or restricting the practice of the activity or profession for a period determined by the regulatory authority.
g) Cancelling the license.

The Supervisory Authority may, upon imposing the administrative penalties, may issue an order requesting the submission of the regular reports on the measures taken to address the violation.

The supervisory authority may impose an increased administrative fine in the event of a recurrence of the same violation within a period not exceeding one year from the date of imposing the administrative fine for the previous violation.

In all cases, the supervisory authority may publish the administrative penalties it imposes in various publication media.

The mechanism for sharing administrative fines issued by local supervisory authorities shall be determined by a decision of the Council of Ministers based on the recommendation of the Minister.

Vide Cabinet Decision 16 of 2021; the MOE is empowered to impose the following administrative fines.

- **3 contraventions** with a fine of **AED 1 million each**.
    1- Dealing with fake banks in all ways.
    2- Opening or maintaining bank accounts with fake names or numbers without the names of their owners.
    3- Failure to take measures related to clients listed on international or domestic sanctions lists, prior to establishing or continuing a business relationship.

- **5 contraventions** with a fine of **AED 200,000 each.**:
    1- Failure to take enhanced due diligence measures to manage high risks clients.

2- Not notifying the Financial Intelligence Unit of a suspicious transaction report when it is not possible to take due diligence measures towards a client before establishing or continuing a business relationship with him or carrying out a transaction for the benefit of the client or in his name.
3- Failure to respond to the additional information request by the GoAML regarding the suspicious transaction report that has been filed.
4- Disclosure, directly or indirectly, to the customer or to others about reporting the customer or the intention to report to him, on suspicion of the nature of the business relationship with him.
5- Failure to implement the measures set by the National Committee to Combat Money Laundering regarding clients from high-risk countries.

- **7 contraventions** with a fine of **AED 100,000 each**:
  1- Failure to take the necessary measures to determine the risks of crime in one's field of work.
  2- Failure to identify and assess risks that may arise in his field of work when he develops the services he provides or undertakes new professional practices through his establishment.
  3- Failure to take due diligence measures towards clients before establishing or continuing a business relationship or carrying out a process in the name of or for the benefit of the client.
  4- Failure to verify - using documents or data from a reliable and independent source - the identity of the customer and the real beneficiary or someone their behalf before establishing a business relationship or account opening or during them, or before carrying out a process for a client with whom he has no existing business relationship.
  5- Delayed reporting on GoAML of a suspicious transaction report if there is suspicion or are reasonable grounds to suspect that the business relationship with the customer is linked to the crime in whole or in part, or that the client's money that is the subject of the business relationship from the proceeds of a crime or used in it.
  6- Failure to apply due diligence measures towards politically exposed clients before establishing or continuing a business relationship.
  7- Not creating records to keep track of financial transactions with clients.

- **11 contraventions** with a fine of **AED 50,000 each**:
  1- Failure to take necessary measures and procedures to reduce the identified risks according to the results of the national risk assessment, or the results of the self-assessment given the nature and volume of its work.
  2- Failure to set internal policies, procedures and controls at the facilities aimed at combating the crime or engaging in a suspicious business relationship.
  3- Failure to take simplified due diligence measures to manage low risk.
  4- Failure to take the necessary measures to understand the purpose and nature of the business relationship, or failure to seek to obtain information related to this purpose when needed.
  5- Failure to take the necessary measures to understand the nature of the client's business, the ownership structure of his business, and the extent of the client's control over it.
  6- Failure to take due diligence measures of continuous monitoring towards clients during the business relationship.
  7- Failure to appoint a compliance officer.

8- Create records for keeping financial transactions with clients in an irregular manner that does not allow data analysis and tracking of financial operations.
9- Failure to keep records of financial transactions and documents related to them for a period of five years from the date of completion of the process or the termination of the business relationship with the customer or from the date of the end of the inspection process of his facility.
10- Failure to provide information related to customer due diligence and continuous monitoring and results of their analysis, as well as their records, files, documents, correspondence, and forms to the concerned authorities upon their request.
11- Failure to train employees at his facility on countering money laundering and combating terrorism financing.

However, imposing the above administrative fine shall not limit the MOE's authority to impose any of the other administrative penalties.

12. TRAINING

The Company shall implement a training program for all persons involved in the AML-CFT-CPF and Responsible Supply Chain process, which shall include regular annual training and refresher sessions for new staff, existing staff and management, to be conducted based on the level of risks and job profiles in engaging with the supply chain participants such as:

Low Risk Staff consist of employees not facing clients or not handling transactions such as smelters, assayers, etc.

High Risk Staff consist of the ones facing clients, handling transactions, such as sales staff, valuables handling staff etc.

The Compliance Officer shall be responsible for the implementation of an adequate training program. The Company shall ensure that the training obligations of the Compliance Officer as per the Cabinet Decision, MOE Due Diligence Regulations for Responsible Sourcing of Gold and EBC RBDG Rules are incorporated into this training program.

13. GRIEVANCE MECHANISM

The Company has also established a Grievance Mechanism as an integral part of the AML-CFT-CPF systems & controls, for internal and external stakeholders to be able to voice concerns relating to **The Company**'s risk management processes and AML-CFT-CPF policy to senior management. Any grievance received shall be escalated to the Compliance Department, who shall assess the appropriate response, and shall recommend the necessary measures to mitigate and monitor any identified risks. Depending on the intensity of the grievance, the Compliance Department may also escalate the matter further to the Management.

APPENDIX 1 – EMPLOYEE UNDERTAKING

To,
The Compliance Officer
Emirates minting Factory L.L.C

Dear Sir/Madam,

I confirm that I have read and understand **the Company**'s below-mentioned updated Policies & Procedures.

1. Anti Bribery and Corruption Policy (Document # EMF.POL.CP-01)
2. AML-CFT Policy Manual (Document # EMF.POL.CP-02)
3. General AML-CFT COMPLIANCE POLICY (Document # EMF.POL.CP-03)
4. Grievance Mechanism (Document # EMF.POL.CP-04)
5. Responsible Sourcing & Supply Chain Policy (Document # EMF.POL.CP-05)

and I do hereby undertake:

a. To familiarize myself with, and always comply with, the principles, standards, requirements, and procedures set out in the Policies & Procedures and, in case of doubt, to consult the Compliance Officer.
b. To act and conduct myself in conformity with the Policies & Procedures and instructions issued by the management from time to time relating to Anti-Money laundering, counter-terrorism financing & Proliferation, and sanctions screening to ensure compliance with UAE Federal AML/CFT/CPF legislation, and other applicable laws.
c. To report any transactions or activities which I find suspicious to the Compliance Officer in accordance with Internal STR/SAR reporting procedures.
d. To keep all information relating to SAR/STR reporting confidential; and
e. To make myself readily available in accordance with instructions issued by the management for the purposes of any inspection, investigation, any process or proceeding.

I agree that this undertaking extends to any amendment or replacement to the Policies & Procedures and any other relevant documents that **the Company** subsequently circulates from time to time.

I understand and acknowledge that breaches of the above undertaking may be treated as serious misconduct warranting a disciplinary action including summary dismissal.

Name: .....

Designation: .....

Date: ..... Signature: .....

EMIRATES MINTING

APPENDIX 2 – COMPLIANCE PROCEDURES & FORMS

Name of Procedure	Document #
Anti Bribery and Corruption Policy	EMF.POL.CP-01
Anti-Money Laundering, Counter-Terrorism Financing, and Sanctions screening Policies & Procedures Manual	EMF.POL.CP-02
General AML-CFT COMPLIANCE POLICY	EMF.POL.CP-03
Grievance Mechanism	EMF.POL.CP-04
Responsible Sourcing & Supply Chain Policy	EMF.POL.CP-05
Account Opening Procedure & forms	CP-01
Risk Assessment Procedure & forms	CP-02
Enhanced Due Diligence Procedure & forms	CP-03
Physical Gold Shipment Receipt Procedure & forms	CP-04
Updating KYC Records Procedure & forms	CP-05
Internal Audit Procedure & forms	CP-06
Records Management Procedure & forms	CP-07
Trainings and Communication Procedure & forms	CP-08
Policy Review Procedure	CP-09
Document Control Procedure & forms	CP-10
Cash Payment Procedure & forms	CP-11
Internal Transfer (Funds-Gold) Procedure & forms	CP-12
Cheque Payment Procedure & forms	CP-13
Wire Transfer Payment Procedure & forms	CP-14
Inward Payment Receipt Procedure & forms	CP-15
Physical Gold Delivery Procedure & forms	CP-16
Suspicious Transaction Identification and (Internal-External) Reporting Procedure & forms	CP-17
Targeted Financial Sanctions Screening & Reporting Procedure	CP-18
Management Reporting Procedure	CP-19

APPENDIX 3 – INDICATORS OF SUSPICIOUS TRANSACTIONS (RED-FLAGS)

The Counterparty, or Customer-

- Suddenly cancels the transaction when asked for identification or information.
- Is it reluctant or refuses to provide personal information, or Emirates Minting Factory L.L.C has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
    - their business activities and corporate history.
    - the identity of the beneficial owner.
    - their source of wealth/funds.
    - Why they are conducting their activities in a certain manner.
    - Who are they transacting with; the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions)?
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Is a designated person or organization (i.e. is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Is a foreign national with no significant dealings in the UAE, and no clear economy or other rationale for doing business with Emirates Minting Factory L.L.C.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping gold into ordinary-looking items, or re-cutting and polishing precious stones) that could improperly disguise the nature of the transaction or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.
- Claims to be a legitimate precious metals dealer but cannot demonstrate history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others).

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

The transaction:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of precious metals (especially diamonds and gold) or Jewellery for cash in small incremental amounts.
- Involves the barter or exchange of precious metals (especially diamonds and 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.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves precious metals 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.
- Involve people residing in tax havens or High-Risk Countries when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involve several successive transactions which appear to be linked, or which involve the same parties or those people who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal people 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 completes in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties:
  - ✓ Do not show particular interest in the details of the transaction.
  - ✓ Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms; or
  - ✓ Insist on an unusually quick completion, without a reasonable explanation.
- It takes place through intermediaries who are foreign nationals or individuals who are non-residents for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licenses, or other official requirements.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g., false entries on bills of lading); or multiple trading of the same goods and services).

Means of payment:

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

EMIRATES MINTING

APPENIDX 4 - INTERNAL SUSPICIOUS ACTIVITY REPORTING FORM

1.	**Submission details:**	
Date:		Submitting Employee Name:
Submitting Employee Contact:		Submitting Employee Email:
2.	**Details of the person/s of interest (POI)/ Suspect or associates related to the transaction**: If the POI is a natural person fill Part 2, If POI/ Suspect is a legal person/arrangement fill Part 3. If the POI / Suspect involves both natural and legal person/arrangement fill both Part 2 and 3.	
Person of Interest: Provide as much details as you know about the POI/ Suspect and include copies of any identification documents obtained		**Nationality and Residency Information** ☐ UAE Local ☐ Resident/Expat ☐ Non-Resident Nationality (if non-Resident): EID / ID No.: Passport No.:
Person of Interest: Personal Info and Contact Details		Name: DOB: Gender: Mobile No: Phone No: Email: Occupation: Employer Name: Employer Address: Employer Phone No: Employer Email: Any Other Personal Information:
3.	**Suspected Legal Person/Arrangement**	
Name of legal person/arrangement:		
Type of legal person/arrangement:		☐ Private Company ☐ Public Company ☐ Partnership

	☐ Trust or similar legal arrangement ☐ Other Specify:
Which jurisdiction is the legal person/arrangement registered?	
Registration No. of the legal person/arrangement:	
Registered address:	
Operational address, if different from registered address:	
Legal person/arrangement contact details:	Phone No: Mobile No: Email: Other information:
Beneficial Owner of the legal person/arrangement.	Name: Phone No: Mobile No: Email: Other information:
Reason for association if the person of interest (POI)/ Suspect is other than BO.	☐ Manager/Director ☐ Partner ☐ Signatory ☐ Power of Attorney ☐ Other: Specify:

4.	**Details of the suspicious transaction/activity**
When did this suspicious transaction/activity occur?	Date:
Where did this suspicious transaction/activity occur?	
How was the suspicious transaction/activity identified?	☐ Face to face transaction ☐ Compliance Officer or MLRO ☐ Anonymous Tip ☐ Internal Audit ☐ Negative News ☐ Other Specify:

No. of transactions suspected	☐ One Transaction ☐ Multiple Transactions
What is the suspected value of the transaction/s, including any attempted transaction?	☐ Value in AED: ☐ Value in Other Currencies:
What type of fund, service or product was used for the transaction?	☐ Cash ☐ Cheque ☐ Wire transfer ☐ Bank account ☐ Currency exchange ☐ Gold or Silver Bars ☐ Other precious metal ☐ Diamonds ☐ Other Precious stones ☐ Other:
Provide a detailed narrative about the actual suspicious activity resulting in the filling of this internal STR/SAR form. What raised your suspicions? Describe clearly and completely the factors or unusual circumstances that led to the suspicion of ML or TF activity.	
Provide any additional information that you consider important to file this internal STR/SAR.	
Please list any supporting documents attached and relevant to the filing of this STR/SAR.	☐ POI/ Suspect Identification documents ☐ Transaction records ☐ Company/business records ☐ Any other documents or records List:

PLEASE SEND THIS COMPLETED FORM WITH SUPPORTING DOCUMENTS TO THE MLRO.
Employee Name:
Date:
Signature:
COMPLIANCE OFFICER ACKNOWLEDGMENT
Compliance Officer Name:
Date:
Signature:
Remarks: