# POLICIES AND PROCEDURES MANUAL FOR COMPLIANCE, ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING

## Emirates Gold DMCC

1. Acronyms and their Full Forms ..... 5
1.1 Glossary of Terms Used in the AML/CFT Policy and Procedures ..... 6
3.0 Definition of money laundering, financing of terrorism, and proliferation financing ..... 10
3.01 Money Laundering ..... 10
3.02 Financing of Terrorism ..... 11
3.03 Proliferation Financing ..... 12
4.0 AML/CFT Legal and Regulatory Framework ..... 12
5.0 Commitment statement ..... 13
6.0 Scope of Application ..... 14
7.0 Policy Custodian ..... 14
8.0 Periodical Review ..... 15
9.0 Emirates Gold DMCC's Services ..... 15
10.0 Governance Framework ..... 15
10.01 Three Lines of Defence ..... 15
10.02 AML/CFT Governance Elements ..... 16
10.02.01 Responsibilities of Senior Management ..... 16
10.02.02 Policy Governance ..... 17
10.02.03 Responsibilities of the Senior Management along with Compliance Department for AML/CFT ..... 17
10.02.04 Role of the Key Members of the Senior Management along with Compliance Department for AML/CFT ..... 18
10.02.05 Staff Training & Screening ..... 20
10.02.06 Independent Audit Function ..... 20
11.0 The identification and assessment of ML/FT & PF risks ..... 21
11.01 Entity-Wide Risk Assessment ..... 21
11.02 Risk-Based Approach ..... 21
11.03 Risk Factors ..... 22
11.03.01 Risks Associated with Precious Metals and Stones ..... 22
11.03.02 Features of DPMS that Increase Risk ..... 23
11.03.03 Regulatory Environment ..... 23
11.03.04 Products, Services, and Delivery Channels Risk ..... 23
11.03.05 Customer or Business Relationship Specific Risk ..... 23
11.03.06 Geography Risk ..... 23
11.03.07 ML/TF/PF Risks to be considered by Emirates Gold ..... 24
11.04 Risk Assessment ..... 24
12.0 Customer Due Diligence ..... 25
12.01 Circumstances and Timing for Undertaking CDD ..... 26

12.01.01 Business Relationship ..... 26
12.01.02 Occasional Transaction ..... 27
12.01.03 Handling exceptional circumstances ..... 27
12.02 Identity Verification ..... 27
12.03 Customer Onboarding ..... 28
12.03.01 Natural Persons and Individual Members of Corporate Customers ..... 28
12.03.01 Legal Persons ..... 29
12.03 Risk Profiling ..... 30
12.04 KYC Process ..... 30
12.05 High-Risk Customers and Enhanced Due Diligence ('EDD') Measures ..... 31
12.05 Politically Exposed Persons (PEPs) ..... 31
12.06 Sanctioned Individuals/Entities ..... 32
12.07 Ongoing Monitoring of Business Relationship ..... 32
12.06 Reliance on third parties for CDD ..... 32
12.08 Customer Acceptance Policy ..... 32
12.09 Customer Exit Policy ..... 33
12.10 Cash Acceptance Policy ..... 33
13.0 Indicators of suspicious activities – red flags ..... 34
14.0 Reporting of Suspicious Transactions/Activities ..... 37
14.01 Types of Reporting on the goAML portal ..... 38
14.01.01 Funds Freeze Report (FFR) ..... 38
14.01.02 Partial Name Match Report (PNMR) ..... 38
14.01.03 Suspicious Transaction/Activity Reporting (STR/SAR) ..... 38
14.01.04 High-Risk Countries Report / Activity (HRC/HRCA) ..... 40
14.01.05 Dealers in Precious Metals & Stones Report (DPMSR) ..... 40
14.01.06 Tipping Off and Confidentiality ..... 40
15.0 International Financial Sanctions ..... 41
15.01 Targeted Financial Sanctions ..... 41
15.02 Other International Sanctions ..... 43
15.02.01 The United States of America ..... 43
15.02.02 The European Union ..... 43
15.02.03 The United Kingdom ..... 43
16.0 Training and Awareness ..... 44
17.0 Record-keeping and Record Retention Policy ..... 44
APPENDIX A - AML/CFT Legal and Regulatory Framework ..... 46
National Legislative and Regulatory Framework ..... 46

**International Legislative and Regulatory Framework**.....47

## 1. Acronyms and their Full Forms

| | |
|---|---|
| AML | Anti-Money Laundering |
| AMLD | Anti-Money Laundering and Combatting the Financing of Terrorism Supervision Department |
| CBUAE | Central Bank of the UAE |
| CO | Compliance Officer |
| CDD | Customer Due Diligence |
| CFT | Combatting the Financing of Terrorism |
| CoP | Code of Practice |
| DMCC | Dubai Multi Commodities Centre Authority |
| DNFBPs | Designated Non-Financial Business and Professions |
| DPMS | Dealers in Precious Metals and Stones |
| EDD | Enhanced Due Diligence |
| EOCN | Executive Office for Control and Non-Proliferation |
| EU | European Union |
| FATF | Financial Action Task Force |
| FIU | Financial Intelligence Unit |
| FT | Financing Terrorism |
| ID | Identification |
| INTERPOL | International Police Organisation |
| KYC | Know Your Customer |
| LBMA | London Bullion Market Association |
| MENAFATF | The Middle East and North Africa Financial Action Task Force |
| ML | Money Laundering |
| MLRO | Money Laundering Reporting Officer |
| NAMLCFTC | National Committee for Combatting Money Laundering and the Financing of Terrorism and Illegal Organisations |
| OECD | Organisation for Economic Co-operation and Development |
| OFAC | Office of Foreign Assets Control |
| PEP | Politically Exposed Person |
| PF | Proliferation and Proliferation Financing |
| PMS | Precious Metals and Stones |
| RJC | Responsible Jewellery Council |
| SAR | Suspicious Activity Report |
| STR | Suspicious Transaction Report |
| VR | Verification |
| UAE | United Arab Emirates |
| UBO | Ultimate Beneficial Owner |
| UN | United Nations |

## 1.1 Glossary of Terms Used in the AML/CFT Policy and Procedures

| Term | Definition |
|---|---|
| **Beneficial Owner** | A natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or the natural person who exercises effective ultimate control over a legal person or Legal Arrangement, whether directly or through a chain or ownership, control or other indirect means. |
| **Business Relationship** | Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them. |
| **CBUAE** | Central Bank of the United Arab Emirates. |
| **CFT** | Combating the Financing of Terrorism {this document shall use the Financing of Terrorism (FT) and Combating the Financing of Terrorism (CFT) interchangeably with no risk of confusion}. |
| **Customer** | Any person involved in or attempts to carry out any of the activities specified in the Executive Regulations of this Decree-Law with one of the Financial Institutions or designated non-financial businesses and professions or Virtual Asset Service Providers. |
| **Committee** | National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations. |
| **Competent Authorities** | The competent government authorities in the State entrusted with the implementation of any provision of the Decree-Law and the present Decision. |
| **Confiscation** | Permanent expropriation of private funds or proceeds, or instrumentalities by a ruling issued by a competent court. |
| **Controlled delivery** | The process by which a competent authority allows the entering or transferring of illegal or suspicious funds or crime revenues to and from the State for the purpose of investigating a crime or identifying the identity of its perpetrators. |
| **Customer Due Diligence** | Process of identifying or verifying the information of a customer or Beneficial owner, whether a natural or legal person or a Legal Arrangement, the nature of its activity, the purpose of the business relationship, the ownership structure, control over it for the purpose of this Decree-Law and its Executive Regulation. |
| **Decree-Law (or "AML-CFT Law")** | Federal Decree-Law No. (10) of 2025 On Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Financing. |
| **AML-CFT Decision (or "Cabinet Decision or Cabinet Resolution")** | The Cabinet Resolution No. (134) of 2025 Concerning the Executive Regulations of Federal Decree-Law No. (10) of 2025 concerning combating money laundering, terrorist financing and the financing of the Proliferation of Weapons repeals the Cabinet Resolution No. (10) of 2019. |
| **Designated Non-financial Businesses and Professions (DNFBPs)** | Anyone who conducts one or several of the commercial or professional activities defined in Article (3) of the new Cabinet Resolution No. (134) of 2025 in the UAE. |
| **Egmont Group** | The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/FT). |
| **FATF** | The Financial Action Task Force is an inter-governmental body that sets international standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. |

| | |
|---|---|
| **FSRBs** | FATF-Style Regional Bodies are regional intergovernmental organisations that promote and assess the implementation of internationally accepted AML/CFT policies and regulations. |
| **Financial Transactions or Activities** | Any activity or transaction defined in Article (2) of the present Decision. |
| **Financing of Illegal Organisations** | Any physical or legal action aiming at providing funding to an illegal organisation, or any of its activities or members. |
| | |
| **FIU** | Financial Intelligence Unit. |
| **Freezing or seizure** | Temporary attachment over the moving, conversion, transfer, replacement, or disposition of funds in any form, by an order issued by a competent authority. |
| **Funds** | Assets, whatever the method of acquisition, type and form, tangible or intangible, movable or immovable, electronic, digital or encrypted, including local and foreign currencies, legal documents and instruments of whatever form, including electronic or digital form that proves ownership of such assets, shares or related rights and economic resources that are assets of any kind, including natural resources, as well as bank credits, cheques, payment orders, shares, securities, bonds, bills of exchange, letters of credit, and any interest, profits or other incomes derived or resulting from these assets, and can be used to obtain any financing or goods or services. |
| **Governor** | Governor of the Central Bank |
| **High-Risk Customer** | A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority. |
| **Illegal Organisations** | Organisations whose establishment is criminalised or which exercise a criminalised activity. |
| **Law Enforcement Authorities** | Federal and local authorities, which are entrusted under applicable legislation to combat, search, investigate, and collect evidence on crimes, including AML/CFT crimes and financing of illegal organisations |
| **Legal Arrangement** | A relationship established by means of a contract between two or more parties, including but not limited to Trust funds or other similar arrangements. |
| **Local Terrorist List** | The List issued by the Cabinet pursuant to Article (3) of Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions. |
| **MENAFATF** | MENAFATF is a FATF-Style Regional Body (FSRB), for the purpose of fostering cooperation and coordination between the countries of the MENA region in establishing an effective system of compliance with international AML/CFT standards. The UAE is one of the founding members of MENAFATF. |
| **Means** | Any means used or intended to be used to commit a felony or misdemeanour. |
| **Money Laundering** | Any of the acts mentioned in Clause (1) of Article (2) of the Decree-Law. |
| **Non-Profit Organisations (NPOs)** | Any organised group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit, Legal Arrangements for the purpose of collecting, receiving, or |

| | |
|---|---|
| | disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities. |
| **Politically Exposed Persons (PEPs)** | Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which includes: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP. |
| **Predicate Offense** | Any act constituting an offense or misdemeanour under the applicable laws of the State, whether this act is committed inside or outside the State, when such act is punishable in both countries. |
| **Proceeds** | Funds generated directly or indirectly from the commitment of any felony or misdemeanour, including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds. |
| **Proliferation and Proliferation Financing** | Proliferation and Proliferation Financing (PF) mean the threat posed by weapons of mass destruction (WMD) and their associated delivery systems is a distinct but related concept from the financing of such activity. Although the FATF has not presented official definitions of "proliferation" and "proliferation financing", the FATF's 2021 Guidance on Proliferation Financing Risk Assessment and Mitigation offers the following working definitions:<br>• WMD Proliferation refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both Dual-Use technologies and Dual-Use goods used for non-legitimate purposes).<br>• The Financing of Proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both Dual-Use technologies and Dual-Use goods for non-legitimate purposes). |
| **RBA** | A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk. |
| **Sanctions List** | A list wherein individuals and terrorist organisations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee, are listed, along with their personal data and the reasons for Listing. |
| **Settlor** | A natural or legal person who transfers the control of his/her funds to a Trustee under a document. |
| **Shell Bank** | Bank that has no physical presence in the country in which it is incorporated and licensed and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. |

| | |
|---|---|
| **Supervised institutions** | Financial institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) that fall under the scope of UAE AML/CFT Laws (Federal Decree-Law No. (10) of 2025 and Cabinet Resolution. |
| **Supervisory Authority** | Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and non-profit organisations, or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislation. |
| **Suspicious Transactions** | Transactions related to funds for which there are reasonable grounds to believe that they are earned from any felony or misdemeanour or related to the Financing of Terrorism or illegal organisations, whether committed or attempted. |
| **TFS** | Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction. |
| **Transaction** | All disposal or use of Funds or proceeds, including, for example, deposit, withdrawal, transfer, sale, purchase, lending, swap, mortgage, and donation. |
| **Trust** | A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor. |
| **Trustee** | A natural or legal person who has the rights and powers conferred upon him by the Settlor or the Trust, under which he administers, uses, and acts with the funds of the Settlor in accordance with the conditions imposed on him by either the Settlor or the Trust. |
| **Virtual Assets (VA)** | A digital representation of the value that can be digitally traded over transferred, and can be used for payment or investment purposes, and otherwise, as specified in the Executive Regulation of this Decree-Law. |
| **Virtual Assets Service Providers (VASP)** | Any natural or legal person who practices any kind of commercial business, conducts one or more of the activities of virtual assets specified in the Executive Regulation of this Decree-Law, or the operations related thereto for the benefit or on behalf of another natural or legal person. |

## 2. Purpose and Rationale

The purpose of this Policy is to set out provisions, procedures and controls as enacted by Emirates Gold DMCC (also referred to as "Emirates Gold", "the Company") concerning Anti-Money Laundering ("AML") and Combating the Financing of Terrorism (CFT) and Proliferation Financing (PF). All relevant personnel at Emirates Gold must be aware of its existence and the contents within the Policy and hold the personal and corporate responsibility to bring any AML/CFT concerns to the attention of the Compliance Officer.

The rationale behind the Policy is unequivocally clear. The Company will only accept those Business Relationships:

- Whose sources of funds can be reasonably established as legitimate;
- Whose ultimate beneficial ownership is transparently verified; and
- Who do not pose any risk (actual or potential) to Emirates Gold's reputation and commitment towards AML/CFT.

The Company will also ensure that all its staff are aware of the Policy and its contents, including the penalty for any non-compliance, and will not tolerate any involvement in illegal activities.

The Company will cooperate fully and timely with the competent supervisory authorities — including the Ministry of Economy, FIU, or other regulators as and when required.

## 3.0 Definition of money laundering, financing of terrorism, and proliferation financing

The emergence of rapid globalization and accelerating technological disruption within recent years has caused money laundering and financing of terrorism to become an issue of unprecedented magnitude. Every day, organizations across the globe encounter new threats due to their global presence and vast diversity of products, services, markets, business lines, and distribution channels. The interconnectedness and integration of the global financial and trade system, ever-changing payment methods, and fewer restrictions on the movement of human capital have given rise to a whole new range of sophisticated methods for criminals to launder money and finance terrorism. As a result, businesses face increased regulatory scrutiny, higher compliance costs, and the need to continuously adapt their risk management frameworks to prevent financial crime. Non-compliance with evolving regulations can lead to severe legal, financial, and reputational consequences, including hefty fines, operational disruptions, and loss of customer trust. The need to be more vigilant on an international level has arisen, requiring coordinated and coherent efforts at various levels to protect the integrity and stability of the international financial system. Businesses must implement robust anti-money laundering (AML) and counter-terrorist financing (CTF) measures, invest in advanced technology solutions, and foster a culture of compliance to mitigate risks effectively. Strengthening internal controls and collaborating with regulatory bodies and industry peers has become essential to cutting off the resources available to terrorists and making it more difficult for those engaged in crime to profit from their illicit activities.

### 3.01 Money Laundering

A person shall be deemed to have committed money laundering if that person knows or there are sufficient indications or evidence to believe that the Funds, in whole or in part, are the proceeds of a Predicate Offence, and intentionally commits any of the following acts:

a) Converts, transfers, or carries out any transaction involving the Proceeds for the purpose of concealing or disguising their illicit origin.

b) Conceals or disguises the true nature of the proceeds, source, location, disposition, movement, ownership, or rights related thereto.
c) Acquires, possesses, or uses the proceeds upon receipt thereto.
d) Assists the perpetrator of the Predicate Offence in evading punishment therefor.

Federal Decree-Law No. (10) of 2025 replaced the 2018 AML Law with a broader mandate to combat money laundering, terrorist financing, and proliferation financing (PF). As per the new AML law, money laundering involves intentionally dealing with illicit proceeds (from any serious crime) by converting, concealing, acquiring, or transferring them, with increased penalties ranging from AED 5 million to AED 100 million for companies and imprisonment up to 10 years for individuals, covering virtual assets and digital systems, and emphasizing greater corporate accountability with potential dissolution, aiming to align with global standards. Beyond traditional ML/TF, the 2025 law explicitly adds proliferation financing, virtual assets, digital/ encrypted systems – meaning new business lines and technology channels must be assessed for risk.

- **Stages of Money Laundering**

Despite money laundering being a rather complex series of transactions, which are difficult to separate, it can be simplified into commonly consisting of three primary stages:

1. **Placement:** This is the first stage in separating the illicit funds from their illegal source. During this phase, the initial proceeds that are derived from illegal activities are introduced into the financial system through typically, placing the funds into circulation through formal financial institutions, casinos, the real estate sector, the gold and precious metal industry, restaurants, and other legitimate businesses, both domestic and international.
2. **Layering:** Once the proceeds from the illicit activities have entered the financial system, the next stage in the process involves converting the illegal funds into another form, creating complex layers of financial transactions to conceal the original source and ownership of the funds. This makes it difficult to associate the illegal funds with the predicate crime.
3. **Integration:** This is the third stage that completes the money laundering cycle. By this stage, the laundered funds appear to be legitimate, and it is exceedingly difficult to distinguish between legal and illegal wealth. These integration schemes are done to ensure that laundered proceeds are placed back into the economy in what appear to be normal business or personal transactions.

## 3.02 Financing of Terrorism

Financing of Terrorism is also a three-step process of collecting, transmitting, and distributing funds for terrorist activities. This involves raising money, either through illegal or legal channels, and then laundering it through the financial system to conceal its origin and destination. Finally, the laundered funds are distributed to terror cells, who use them to purchase weapons, pay for supplies, or otherwise advance the group's goals. Terrorists regularly adapt how and where they raise and move funds and other assets to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity.

The AML/CFT Law defines Financing of Terrorism as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organisation or terrorist person or intended to finance a terrorist

organisation, a terrorist person, or a terrorism crime, even if it is without the intention to conceal or disguise their illicit origin;

- Providing, collecting, preparing, or making funds available (directly or indirectly, including via digital means) with knowledge they will be used for terrorism, regardless of source or if linked to a specific act.

### 3.03 Proliferation Financing

The UAE's 2025 Federal Decree-Law No. (10) significantly updates its anti-financial crime framework, replacing the focus on "Illegal Organisations" with "Proliferation Financing" (of Weapons of Mass Destructions /arms) and broadening scope to include Virtual Assets, Terrorism Financing, and Tax Evasion. The new law explicitly incorporates Proliferation Financing , making it a standalone offence, alongside combating terrorism and money laundering.

## 4.0 AML/CFT Legal and Regulatory Framework

The United Arab Emirates (UAE) is fully committed to combating money laundering and terrorism financing, as well as detecting and deterring them in accordance with established legislation. The competent authorities have implemented an institutional system to oversee, control, and collect information on all practices that may lead to financial crimes, including money laundering and terrorism financing.

Underpinned by its commitment to safeguard the UAE's fiscal landscape from illegal financing and corruption, the National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee (NAMLCFTC) was established in 2000 to oversee anti-money laundering national strategies and develop policies in the UAE. Specifically, the Committee serves to enhance the effectiveness of the AML/CFT framework in the UAE by ensuring continuous adherence to international standards related to combating money laundering and terrorist financing crimes.

In 2018, the Executive Office of AML and CFT was established as the key coordinating body responsible for overseeing and implementing the country's efforts, serving as the administrative and operational arm of the NAMLCFTC.

In August 2020, the Central Bank of the UAE (CBUAE) established a dedicated department, the Anti-Money Laundering and Combatting the Financing of Terrorism Supervision Department (AMLD), to handle all AML/CFT matters. Through AMLD, the CBUAE coordinates closely with the UAE's National AML/CFT Committee to implement the National Action Plan effectively.

As part of the 2024 reforms, the National Committee for Anti-Money Laundering and Combating the Financing of Terrorism (NAMLCFTC) underwent restructuring, now supported by the newly established Supreme Committee for the Oversight of the National Strategy for AML/CFT and the General Secretariat, which replaced the Executive Office. This reorganisation has facilitated greater coordination across sectors and strengthened the implementation of a unified strategy. The Supreme Committee provides overarching guidance to ensure that the UAE's AML/CFT strategy is comprehensive, adaptive to emerging risks, and consistent across all governmental and private sector initiatives. Meanwhile, the General Secretariat was created with a broader mandate to coordinate the administrative work that supports NAMLCFTC's activities, ensuring smoother execution of AML/CFT regulations and enhancing coordination with key entities.

In 2025, the UAE issued Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing, further strengthening the legislative

foundation for AML/CFT and expanding regulatory powers to address evolving risks, including virtual assets and proliferation financing.

Following the introduction of the new AML Law, the United Arab Emirates Cabinet issued Cabinet Decision No. 134 of 2025 (the "Executive Regulations") alongside it. The Executive Regulations repealed and replaced Cabinet Decision No. 10 of 2019 and introduced an expanded and modernised compliance framework for Financial Institutions and DNFBPs. It codifies enhanced obligations for ultimate beneficial ownership transparency, tighten controls for Virtual Asset Service Providers and virtual asset transfers and expand the powers of supervisors including the Financial Intelligence Unit.

## 5.0 Commitment statement

As a responsible organisation registered in the UAE, **Emirates Gold DMCC** is committed to supporting domestic and international efforts to combat money laundering, the financing of terrorism, and other financial crimes. The Company upholds the highest standards of ethical conduct and strict compliance with all relevant laws, regulations, and best global practices in AML/CFT.

Recognising the critical importance of preventing financial crimes, the Company has established robust internal policies and procedures to ensure that its activities are conducted with integrity and transparency. These policies are designed to:

- Align business operations with ethical standards and regulatory requirements,
- Implement monitoring and reporting mechanisms to prevent misuse of the Company's services for illicit activities,
- Enforce Know Your Customer (KYC) procedures and due diligence measures,
- Ensure strict adherence to AML/CFT legislation and international recommendations, including those set by the Financial Action Task Force (FATF) and UAE authorities.

To reinforce this commitment, **Emirates Gold DMCC** is willing to support and actively cooperate with government and law enforcement agencies, both domestic and international, including the UAE Central Bank, the Ministry of Economy, and global regulatory bodies. The Company continually enhances its AML/CFT framework by staying updated on evolving regulations, training employees, and integrating advanced technological solutions to detect and prevent financial crimes.

The Company's team is directly responsible for compliance with regulatory standards and assisting in efforts to combat money laundering and terrorist financing. The Company wants to convey its position on AML/CFT via this Policy Document and to reaffirm that the Company will only conduct business activities in strict compliance with all relevant laws, regulations, and best global practices in the domain of AML/CFT/PF. The Company regards the fight against money laundering and/or counter-terrorist financing as a matter of great importance for the organisation and views it as a collaborative endeavour. The Company's commitment to combatting money laundering and terrorist financing is demonstrated through the publication of this Policy, as well as the implementation and operation of the processes and controls included therein.

The Company's management and employees are responsible for maintaining vigilance and reporting any suspicious activities in accordance with internal policies and regulatory obligations. Compliance with this AML/CFT Policy is mandatory for all employees, and non-compliance may result in disciplinary action.

As an organisation operating in the gold and precious metals sector, **Emirates Gold DMCC** ensures that its procurement, distribution, and trading activities do not contribute to money laundering, terrorist

financing, proliferation financing or serious human rights violations. The Company adheres to internationally recognised guidelines, including:

- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas,
- Ministerial Decree requirements,
- UAE Good Delivery Standards
- UAE Ministry of Economy's Due Diligence Guidelines on Responsible Sourcing of Gold.

Through this commitment, the Company affirms its dedication to uphold global AML/CFT standards and ensuring a secure and compliant business environment for all stakeholders.

## 6.0 Scope of Application

The provisions, procedures and controls detailed below shall apply to:

- All employees, if any, regardless of their function or location of work.
- All clients, including Buyers, Sellers, Refiners, Suppliers, Diamond, Gold & Precious Metals Companies.
- Third parties, including consultants, lawyers, and other external advisors, engaged with Emirates Gold DMCC.

Emirates Gold's employees are responsible for ensuring that they comply with the standards established by local and international regulatory agencies. The firm's employees are further expected to prevent the Company and its reputation from being exploited for any illegal activity.

If any of the Company's employees or affiliates violate the provisions contained within this Policy, such violations will be treated as a disciplinary offence, and the Company reserves the right to take any additional action that it, in its sole discretion and within the permissibility of the law, deems necessary to ensure the diligent and proper implementation and enforcement of this Policy. Additionally, if the Company, its personnel, and/or premises are inadvertently used for money laundering or other illegal activities, the Company can be subject to potentially serious civil and/or criminal penalties. It is imperative that every member, officer, director, and employee of the firm is familiar with and complies with the processes and procedures set forth in this Policy.

If any client of the Company is found to have breached any provisions of this Policy, then Emirates Gold DMCC may take any of the following measures, in accordance with the severity of the violation:

- Warning
- Temporary suspension of the operations of the Client's account
- Termination of the Client's account
- Reporting to the relevant Authorities

## 7.0 Policy Custodian

The MLRO/CO has been designated as the Policy Custodian for Anti-Money Laundering and Combating Financing of Terrorism and Proliferation Financing.

Although the MLRO/CO is the Custodian of the Policy, the Company's management shall have responsibility for the enforcement of this Policy within the organization and with its clients, as well as being responsible for the entirety of the AML/CFT Programme.

## 8.0 Periodical Review

This AML/CFT Policy shall be reviewed on at least an Annual basis. Any review shall take into consideration legislative changes regarding AML/CFT and shall also examine the previous twelve months' implementation of the Policy, how the implementation may be improved, and any subsequent comments made during periodical checks by relevant authorities. Any amendments made to the Policy must have received prior written sign-off from Emirates Gold DMCC's Senior Management, whereupon they shall take effect immediately.

## 9.0 Emirates Gold DMCC's Services

With over 33 years of excellence in Dubai, Emirates Gold DMCC stands as the GCC region's most trusted and influential precious metals refinery. Renowned for its exceptional client service, reputation, and finest-quality products, Emirates Gold has significantly contributed to establishing Dubai as a global leader in the precious metals industry, with support from the Dubai Government.

Specialising in the refining of gold and silver, Emirates Gold offers a diverse range of products, including gold bars, coins, medals, and custom-made items. Its state-of-the-art technology and highly skilled team ensure superior craftsmanship and precision in every product delivered. As a pioneer in the precious metals sector, Emirates Gold holds a leading position with a significant market share. In 2005, it became the first refinery in the Middle East to achieve the prestigious Dubai Good Delivery accreditation, now known as UAE Good Delivery.

Emirates Gold's operations are certified to the highest international standards, including ISO 9001:2015, ISO 14001:2015, and ISO 45001:2018. Committed to delivering pure, high-quality products, Emirates Gold maintains an unwavering focus on excellence and a client-first approach. In September 2024, Emirates Gold was acquired by Bright East Holding 1, a licensed entity with share certificate number SD-416022.

Located at Unit/Plot No: PP-01-1G, Enterprise Zone 1, Al Sarayat Road, Jumeirah Lakes Towers, Dubai, Dubai, United Arab Emirates, PO BOX 24305, +97143679030, the Company possesses two licenses, Trading License-DMCC-31274, and Industrial License-DMCC-30004, and engages in the following licensed activities:

- Non-Manufactured Precious Metal Trading
- Jewellery Trading
- Gold Refinery
- Gold &Precious Metal Casting

Trading License-DMCC-31274

Industrial License-DMCC-30004

## 10.0 Governance Framework

### 10.01 Three Lines of Defence

In a refinery such as Emirates Gold, its Compliance Department acts as a critical defence mechanism by proactively identifying and mitigating potential regulatory breaches and ethical failures, thus safeguarding its business from ML/FT/PF risk and ensuring responsible sourcing of gold.

- **First Line of Defence** – At the refinery, Operations Department and employees directly facing the customers acts as the first line, owning and managing the risks associated with their day-to-day activities, such as sourcing and processing gold. They are responsible for implementing internal controls and policies.

- **Second Line of Defence** – The Compliance Department operates as the second line of defence within the company's governance and risk management framework, providing oversight and guidance to the front-line operations. The key functions of the Compliance Department constitute developing policies and procedures, upholding ethical supply chain practices, identifying, and maintaining potential operational and reputational risks associated with refining activities and ensuring accurate record-keeping of all materials and processes for transparency and regulatory reporting.

- **Third Line of Defence** – This is the third line of defence. This function provides independent assurance to determine if proper controls are established. The Company may appoint an independent compliance internal audit reviewer and external auditor periodically to evaluate the effectiveness of the first and second lines' compliance and control systems, reporting findings to the senior management. In the event of any perceived gaps, the shortfall will be presented to the management, and a remediation action plan will be developed.

## 10.02 AML/CFT Governance Elements

The Company has a Policy to follow the below-mentioned approach to ensure a strong and effective AML/CFT compliance culture in the Company.

### 10.02.01 Responsibilities of Senior Management

Senior Management of the Company is committed to ensuring that an effective AML/CFT compliance programme is in place. Further, the senior management has clearly articulated their expectations about the responsibilities and accountability of all staff members in relation to the AML/CFT compliance programme.

As part of this Policy, the Company has defined the responsibilities of the senior management as under:

- Appointing a qualified AML/CFT Compliance Officer.
- Ensuring a robust and effective independent audit function is in place,
- Putting in place and monitoring the implementation of adequate management and information systems, internal controls, and policies, procedures to mitigate risks,
- Approval of internal policies, procedures, and controls, including customer acceptance,
- Reviewing and providing comments in relation to the CO's semi-annual reports.
- Approving the establishment and continuance of High-Risk Customer Business Relationships and their associated transactions, including those with PEPs,
- Application of the directives of Competent Authorities regarding combating Money Laundering, Terrorism Financing and Proliferation Financing.
- Approval from Senior Management will be required in case of any deviations identified in transactions or during client onboarding.

### 10.02.02 Policy Governance

The Company has established the Compliance Department for overseeing various aspects of its Compliance policy governance, including the coordination and implementation of AML/CFT procedures. Among its wide range of responsibilities, the compliance department is tasked with ongoing monitoring and coordinating the identification, assessment, and mitigation of risks that the Company is or might be exposed to regarding money laundering and terrorism financing. Hence, company ensures that a strong and suitable AML/CFT structure is in place.

In addition to its other responsibilities, the Compliance Department along with members of the Senior Management coordinates efforts to strengthen the Company's AML/CFT framework. The CO on monthly basis at least will conduct a formal scheduled meeting with the Senior Management, to discuss AML/CFT matters, review action plans, and recommend follow-up actions based on the outcomes of the reviews. They shall discuss initiatives required to be undertaken to continually improve the Company's accomplishments within the AML/CFT area.

The CO is responsible for keeping (and safeguarding) minutes of these meetings, detailing the content of the meeting as well as any action points decided (in the "Compliance-Management Meetings").

### 10.02.03 Responsibilities of the Senior Management along with Compliance Department for AML/CFT

The senior management has the overall responsibilities of complying with AML/CFT requirements. For day-to-day conduct of this activities senior management has assigned these responsibilities to the compliance department.

- To prepare a Policy and process manual for implementing the provisions of the UAE's Federal Decree-Law No. (10) of 2025 and Cabinet Decision No. (134) of 2025.
- To ascertain the proper implementation and effectiveness of the procedures and processes for fighting money laundering and terrorism financing operations within the Company.
- To satisfy all its liabilities as a DNFBP.
- To review the above-mentioned procedures and processes on a periodic basis and develop them in line with up-to-date methods and guidance established on combatting money laundering and financing of terrorism.
- To periodically assess the Company's approach to risk identification, assessment, and mitigation plans for the principal legal and regulatory compliance risks facing the company and review the results of it.
- To prepare an effective customer identification and due diligence programme for onboarding a new customer, as well as updating CDD throughout the entire relationship with the customer.
- To periodically review resources, systems, and tools that are available to the Compliance Officer and ensure that they are up-to-date with the current international and national standards and are appropriate to the nature, size, and complexity of the business.
- To review findings of the internal audit and suggest necessary modifications to the Compliance Programme.
- To raise ongoing challenges/issues in the implementation of the AML/CFT procedures and processes and ensure that proper controls are in place to mitigate/solve them.
- To take corrective/preventive actions if any gaps are identified.
- To discuss information about current and emerging legal and regulatory compliance risks and enforcement trends that may affect the Company's business operations, performance, or strategy.

- To review the reports submitted by the Compliance Unit on adopted procedures, unusual operations, and high-risk customers.
- To discuss developing internal programmes focused on promoting an ethical culture within the organisation.
- To review any data suggesting significant non-compliance involving any of the Company's officers or staff. The Compliance Officer, or whoever is acting on their behalf, will report any data suggesting significant non-compliance that could affect the Compliance Programme or the Company.
- To review on a regular basis the company's significant risk exposures or compliance violations and the steps that have been taken to monitor, correct, and/or mitigate such violations or risks.

With reference to periodic meeting of the Compliance-Management, to discuss the following areas and decide whether any actions need to be taken:

- Updates on Sanctions
- Notices / Circulars received from the Regulatory Authority
- Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs) raised.
- Enhanced CDD conducted during the time.
- Training conducted and attendance records of the staff.
- Feedback / Queries received from the Regulatory Authority
- Any new risks associated with AML/CFT that are identified.

### 10.02.04 Role of the Key Members of the Senior Management for AML/CFT

The ultimate responsibility for proper supervision, reporting, and compliance pursuant to AML/CFT shall rest with the Senior Management with assistance from Compliance Department.

The Management will be responsible for the following:

- Responsible for the oversight of all activities at the Company.
- Establishing transparency, honesty, and integrity throughout the business activities.
- Implement a robust compliance program across all its products, services, suppliers, customers, jurisdictions of operation, and delivery channels, including digital and physical transaction platforms.
- To define the procedures and processes to be followed by the senior management team for approving business relationships with high-risk customers or when executing high-risk transactions.
- Ensuring that the Company has in place adequate screening procedures to ensure high standards when appointing or employing officers or employees.
- Approving the overall business risk assessment for the Company.
- Ensuring that all employees of the organisation are being trained on the AML/CFT/PF.
- Preparing, Approving, and Implementation of the Compliance Policy of the Organisation.
- Reviewing any issues identified during the CDD process and resolving them in a timely manner.
- Developing a good knowledge of all applicable Laws, Rules, Regulations, Notices, and the Standards related to the Precious Metals and Stones industry in the UAE.
- Setting the tone of zero tolerance against fraud, money laundering, and terrorism financing.

As part of this Policy, the Company has defined the responsibilities of the AML/CFT Compliance Officer as under:

- **AML/CFT Programme Management**: The CO would be responsible for ensuring the quality, strength, and effectiveness of the Company's AML/CFT programme. The responsibility to oversee the record-keeping requirement as per AML regulations also lies with the Compliance Officer.
- **ML/FT Reporting**: CO would be the Company's suspicious activity/transaction reporting officer as well as the point of contact for communication with the Supervisory Authority and the FIU relating to money laundering issues.
- **AML/CFT Training and Development**: The CO has been entrusted with the responsibility to establish and maintain a strong and effective AML/CFT compliance culture within the Company.

The Company has appointed Mr. Ashwani Singh to act as an authorised Money Laundering Reporting Officer (MLRO) and as the Compliance Officer for the Company. The CO shall avoid the conflict of interest between the day-to-day routine of the Company related to the supply of goods or services and customer business relationship management and shall enthral compliance with independence. The Compliance Offer will be responsible for:

- Creating and implementing the AML/CFT compliance programme for the Company and ensuring compliance with AML/CFT Laws, Regulations, Notices, the Standards, and international laws.
- Establishing and maintaining AML/CFT policies, procedures, processes, and controls in relation to the business of the Company.
- Ensuring compliance by the Company with the provisions of AML/CFT Guidelines, its implementing rules and regulations, and the Company's AML/CFT and KYC Policy.
- Reading any circulars, resolutions, instructions, and policies issued by the UAE Regulatory Agencies in all matters relating to the prevention of money laundering and combatting Financing of Terrorism and Financing of Illegal Organisations.
- Liaising between the Company and UAE Regulatory Agencies in matters relating to compliance with the provisions of the AML/CFT Compliance Guidelines and its rules and regulations.
- Preparing and submitting to UAE Regulatory Authorities written reports on the Company's compliance with the provisions of the AML/CFT Compliance Guidelines and its implementing rules and regulation, in such form as the UAE Regulatory Agencies may determine, and within such period as the UAE Regulatory Agencies may allow in accordance with the AML/CFT Guidelines.
- Attending the compliance training programme, particularly when any laws change.
- Raising Internal Suspicious Transaction alerts, if any, and investigating the matter along with presenting the findings to report all suspicious cases to the FIU.
- Reporting and filing Suspicious Transaction Report (STR) to FIU, if required
- Providing support and assistance to FIU with all the information it requires for fulfilling its obligations.
- Performing more extensive due diligence for high-risk customers and include proactive monitoring for suspicious types of activities.

The Compliance department will be responsible for the following:

- Implementing the Company's Anti-Money Laundering, Combating Terrorist Financing and Proliferation Financing Policy and Procedures.
- Carrying out the compliance officer's role to ensure adherence to the regulations.
- Customer onboarding and KYC documentation.
- Conducting Customer Due Diligence and Enhanced Due Diligence.
- Liaising with other companies to obtain documents and information as required.
- Monitoring day-to-day transactions of the Company for any unusual, structured, suspicious, and blacklisted ones.
- Monitoring of suspicious accounts periodically.
- Reviewing and addressing the watch list and alerts. Update the blacklists regularly.
- Liaising with the compliance department of counterparties.
- Creating sound internal controls and monitoring adherence to them.
- Maintaining records as required by the Company's AML/CFT Policy & Procedures.
- Liaising between the Compliance Officer and the Company regarding Compliance matters.
- Taking proper remedial actions and inform the Compliance Officer if violations are identified.
- Reporting of unusual or suspicious transactions to the Compliance Officer.
- Educating the staff at the Company regarding Anti-Money Laundering & Combating Terrorist Financing and 'Know Your Customer' procedures.

### 10.02.05 Staff Training & Screening

The Company is committed to ensuring that its employees have a clear understanding of the ML/FT risk involved and that the employees are efficient enough to exercise sound judgement to identify suspicious activity and transactions to highlight and report it to the compliance department.

Further, the Company has a Policy to screen every employee before hiring and also before promoting the person to a higher position, to ensure the highest level and quality of AML/CFT compliance.

### 10.02.06 Independent Audit Function

The Company maintains an independent audit function to evaluate the adequacy and effectiveness of its AML/CFT and Responsible Sourcing controls. The audit function provides assurance that the Company's policies, procedures, systems, and internal controls comply with applicable UAE laws, regulatory requirements, and industry standards, including the OECD Due Diligence Guidance and Ministerial Decree 68/2024.

The independent audit function shall be carried out by an internal auditor and an external qualified auditor who is independent of the Compliance Officer and operational teams. The auditor must possess sufficient AML/CFT and Responsible Sourcing expertise.

The responsibilities of the independent auditor include:

- Conducting periodic assessments of AML/CFT documentation, including KYC/CDD/EDD policies and SOPs.
- Testing the effectiveness of AML/CFT controls and processes, including onboarding, screening, monitoring, training, recordkeeping, and suspicious-activity reporting.
- Evaluating the Company's AML/CFT risk assessment, including methodology, risk scoring, and application.
- Assessing the implementation of Responsible Sourcing controls, including supply-chain due diligence and risk mitigation processes.
- Reviewing material inconsistencies, red flags, and escalation procedures.

- Following up on remediation and ensuring corrective actions are closed within agreed timelines.
- Reporting findings directly to Senior Management, ensuring independence and transparency.

The Compliance Officer shall support the audit process by providing documents, data, and access as needed, but shall not perform or influence the independent audit.

## 11.0 The identification and assessment of ML/FT & PF risks

Article 16 of the Federal Decree Law No. (20) of 2020 (which actually stems from the 2018 Law and its amendments) on Anti-Money Laundering and Combating the Financing of Terrorism requires the Company to:

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

As one of the DNFBPs, the Company is required by Federal Decree-Law No. (10) of 2025 and Cabinet Resolution No. (134) of 2025, to identify and assess ML/FT/PF risks. Further, Federal Decree-Law No. 43 of 2021, Cabinet Resolution No. (134) of 2025, Cabinet Resolution No. 50 for 2020, Federal Decree Law No. (10) of 2025 and Cabinet Decision No. (74) of 2020 requires the Company to abide by the legal and regulatory framework for counter-proliferation and its financing. It is the Policy of the Company to assess continuously, document, and update such assessment based on the various risk factors established in the implementing regulation of this Decree-Law and maintain a risk identification and assessment analysis supporting its data.

Further, it is the Company's Policy to document risk assessment operations and keep them up-to-date on an ongoing basis. The Company has adopted a risk-based approach commensurate with the nature and size of its business.

### 11.01 Entity-Wide Risk Assessment

The Company shall conduct an Entity-Wide Risk Assessment (EWRA) also referred to as a Self-Risk Assessment, at least annually, and upon any significant changes in the business or regulatory environment. The EWRA shall evaluate the risks of money laundering and terrorist financing across all business operations, considering factors such as customer profiles, products and services, delivery channels, geographic exposure, and transaction types. It will also identify and assess the risks of unknowingly supporting the spread of Weapons of Mass Destruction and implementing controls proportionate to their PF exposure. The results of the assessment will be used to develop and adjust internal controls, risk mitigation strategies, and resource allocation to effectively manage and reduce identified risks. The assessment process will be overseen by the Compliance Officer and periodically reviewed by senior management to ensure its effectiveness and alignment with applicable UAE laws and regulations.

### 11.02 Risk-Based Approach

The Company adopts a risk-based approach for the identification of ML/FT and PF risks. The objective is to identify, assess, and understand risks in accordance with the nature and size of the Company and based on reasonable grounds after giving due consideration to various risk factors in determining the level of mitigation required. The risk-based approach adopted by the Company allows it to allocate its resources more efficiently and effectively, within the scope of the national AML/CFT legislative and regulatory framework, by adopting and applying preventative measures that are targeted at and commensurate with the nature of the risks it faces.

The assessment of the risk-based approach should be implemented for the overall business, customers, and their due diligence measures, and the training requirements across the Company.

### 11.03 Risk Factors

To implement a risk-based approach to assessing and mitigating risks, it is crucial to identify risk factors. The Company identifies and categorises risks for the application of suitable mitigation measures at the enterprise and customer levels. At the enterprise level, this includes adopting and applying adequate policies, procedures, and controls to business processes. At the customer level, this includes assigning appropriate risk classifications to customers and applying due diligence measures commensurate with the identified risks.

In particular, the precious metals and stones sector offers opportunities for criminals seeking to conceal, transfer, and/ or invest their illicit proceeds. Like cash, 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.

#### 11.03.01 Risks Associated with Precious Metals and Stones

The characteristics of precious metals and stones make them uniquely appropriate as media to store, transfer, and exchange value:

- Precious metals and stones are generally compact, durable, odourless, 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.

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 behaviour:

- Differentiating precious metals and stones often requires laboratory techniques, so it can be difficult or impossible to track their movement.
- Precious metals and stones can be transformed (through re-cutting or recycling) into different objects while retaining their value, interrupting known custody and transfer chains.
- Purchase, sale, and exchange of precious metals often take place outside the formal financial system.

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

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

### 11.03.02 Features of DPMS that Increase Risk

Not all DPMS pose equal risk. A DPMS is likely to be considered 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/combatting the financing of terrorism (AML/CFT) controls.

### 11.03.03 Regulatory Environment

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

In place, but DPMS is 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.

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 the AML-CFT Decision, including the requirement to perform Customer Due Diligence (CDD) and report suspicious transactions.

### 11.03.04 Products, Services, and Delivery Channels Risk

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.

### 11.03.05 Customer or Business Relationship Specific Risk

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

### 11.03.06 Geography Risk

DPMS may be based, or may trade internationally, in jurisdictions that are higher risk for money laundering, the financing of terrorism, and the financing of proliferation. Such DPMS may pose a heightened risk to LFIs. Higher-risk jurisdictions may be characterised 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 terrorists and other non-state armed groups.

- Weak border control measures; and/or
- Sanctions and embargoes

### 11.03.07 ML/TF/PF Risks to be considered by Emirates Gold

When required to apply AML/CFT/PF measures, Emirates Gold should carefully consider factors such as customer risk, geographic risk, channel risk, and product, service, and transaction risk. Consideration should be given to such factors as:

- **Counterparty/customer type, complexity and transparency** (e.g. whether the counterparty or customer is a physical person, a legal person or a legal arrangement; if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a PEP) – particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate.
- **Country of origin of the PMS** - particularly in relation to whether the country is a known production or trading hub for the type of PMS; has adequate regulations and controls; is a High-Risk Country (e.g. is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist organisations).
- **Country of origin or residence status of the counterparty or customer** (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country), particularly in relation to locations where the transaction is 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 (whether physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity.
- **Type, size, complexity, cost, and transparency of both the transaction** (including whether the physical or virtual exchange of merchandise is involved) and the means of payment or financing—particularly in relation to whether they appear to be consistent with the counterparty or customer's socio-economic profile, 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.

The Company has a Policy to properly document the risk assessment, to regularly evaluate and update the same risk factors, and communicate the same with the relevant personnel within the Company.

## 11.04 Risk Assessment

A risk-based approach is one of the most effective ways to protect against money laundering, terrorist financing and proliferation 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.

Customers will be reviewed, assessed, and allocated an appropriate level of risk of money laundering, and the risk assessed shall be in the categories of Low, Medium and High 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** undergo rigorous enhanced due diligence measures when an initial assessment had flagged a customer, transaction or situation as high-risk. The risk level may be downgraded from High to Medium after the EDD process provides additional information that can clarify its profile and mitigate initial concerns. The residual risk (the risk remaining after controls are in place) is considered acceptable within the medium-risk category.
- **Low-Risk customers** may be subject to certain flexibility within the procedures contained in this Policy. However, care should be exercised to ensure that the Company continues to meet its legal obligations.

Although it is generally accepted that failure to provide satisfactory due diligence documentation might be indicative of a money laundering concern, it is also recognised that, due to the geographic diversity of businesses, on occasion, it might prove difficult or impossible to obtain documentation that exactly meets the criteria set out within this Policy.

If the situation mentioned in the Clause above occurs, and there are no reasons to suspect money laundering, the customer documentation should be communicated to senior management and/or the MLRO, together with an explanation detailing the types of issues that arose. Senior management, in consultation with the Compliance Officer, will then review the documentation and consider the risks associated with acceptance of identification evidence that falls outside these procedures, thereafter, providing the personnel with advice and guidance, as appropriate.

The risks considered in the assessment and decision process, and the conclusions reached, should be properly documented within the customer KYC file, with appropriate sign-off by the individuals involved. Only Senior Management, in consultation with the Compliance Officer, may determine the High-risk level to be attributed to any customer or/and approve documentation that does not meet the exact requirements of the Company's Anti-Money Laundering Policy.

All customers are subject to a risk assessment and risk ratings, which will be recorded in the file. Due diligence requirements must be commensurate with the risk level associated with the customer, and enhanced due diligence will be necessary for all higher-risk customers.

In addition to trigger-based reviews, Emirates Gold shall conduct periodic reviews of the Customer's KYC and conduct CDD based on the risk profile of the customer:

- **High-Risk Customers**: Every 12 months
- **Medium-Risk Customers**: Every 12 months
- **Low-Risk Customers**: Every 18 months

If there is no transaction with a particular counterparty for 6 months, then the business relationship status is marked as Inactive, and Re-KYC needs to be performed once the client wants to reinitiate the transaction.

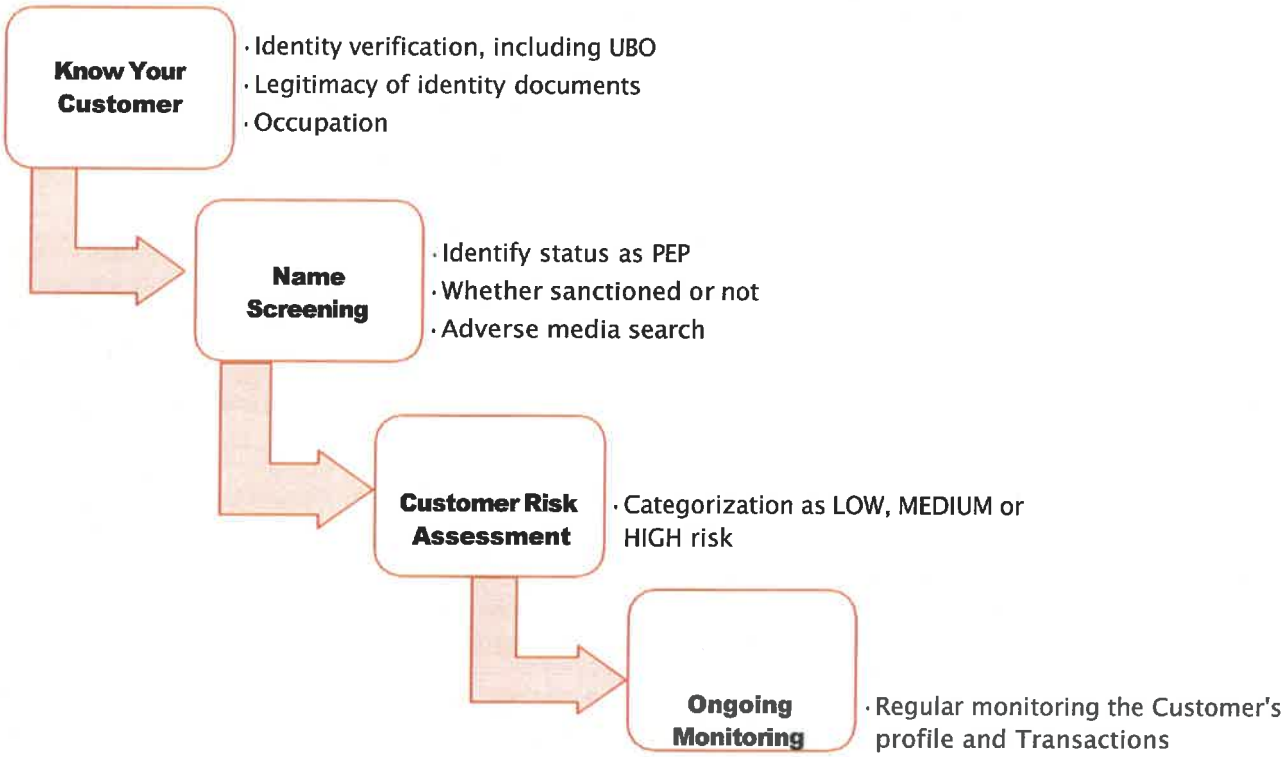
## 12.0 Customer Due Diligence

The Company understands that the risk profile of each customer is dynamic and subject to change depending upon various risk factors, or the discovery of new information, or a change in behaviour or situation. Accordingly, based on the risk identified for a particular customer, the customer due diligence (CDD) level shall be selected as Normal Due Diligence or Enhanced Due Diligence. However, in

certain prescribed conditions, as an exception, the Company shall follow liberal measures under the Customer Due Diligence process.

It is the Policy of the Company to increase the level of due diligence performed for a customer falling under a particular ML/FT/PF risk category whenever the circumstances change, which raises a doubt about the accuracy or appropriateness of the originally designated ML/FT/PF risk category.

The following is the Company's Customer Due Diligence process:




## 12.01 Circumstances and Timing for Undertaking CDD

It is the Company's Policy to verify the identity of the customer or the beneficial owner as a part of the CDD prior to opening the customer's account with the Company for any business relationship or executing a transaction with the customer where there is no business relationship or, say, occasional transactions.

### 12.01.01 Business Relationship

For the above, the Company has defined what shall be construed as a "Business Relationship" as under:

- Effecting any transaction in the customer's name or on their behalf, or at the customer's direction or request for the benefit of someone else,
- Providing any form of tangible or intangible product or service to or on behalf of the customer, or at the customer's direction or request for the benefit of someone else,
- Signing any form of contract, agreement, memorandum of understanding, or other documents with the customer in relation to the performance of a transaction or series of transactions or to

the provision of any form of tangible or intangible product or service as described above,

- Accepting any form of compensation or remuneration (including a deposit or any form of credit) for the provision of products or services,
- Receiving funds or proceeds of any kind from or on behalf of the customer, whether for their account or the benefit of someone else,
- Any other act performed by the Company while conducting our ordinary business, when done on behalf of, or at the request or direction of, a customer.

### 12.01.02 Occasional Transaction

The Company has the Policy and necessary procedures in place to carry out due diligence on all customers, even if they enter transactions occasionally.

### 12.01.03 Handling exceptional circumstances

Though the Company has the Policy to perform the CDD measure before establishing a business relationship or undertaking a transaction with the customer, there may be a few exceptional circumstances where the employees of the Company are allowed to handle the CDD measures differently. We have identified such exceptional scenarios and adequate action in such situations as under:

- When the ML/FT/PF risks identified for the customer are low, and there is no suspicion of criminal activity involved, the customer's identity verification may be completed after establishing the Business Relationship. However, identification verification must be performed before closing the transaction. Moreover, till the time the verification is concluded, the funds shall be held in suspense or an escrow account. Any exception on the said matter shall be approved by the Senior Management or Board of Directors of the company.
- The Company shall not seek any identification information from the publicly listed legal entity or its controlling stakeholders. Rather, the Company shall document the information available from reliable sources such as Stock Exchange disclosure reports or Corporate Annual Report, or Credit Rating agencies' reports.
- In a case where it is suspected that a customer or Beneficial Owner is involved in a crime related to ML/FT or PF and there are reasonable grounds to believe that performing CDD measures would tip off the customer, then the Company has a Policy to directly report the suspicion to the FIU, without applying CDD procedures, along with the reasons why CDD has not been performed.

## 12.02 Identity Verification

The Company has a Policy and necessary procedures in place to identify the customers, suppliers, beneficial owners, beneficiaries, or controlling persons; and verify their identity based on documents and independent sources.

The Company shall obtain and record competent evidence of the true and full identity of the client, Ultimate Beneficiary Owner, representative capacity, domicile, legal capacity, occupation, or business purposes of clients, as well as other identifying information on those clients, whether they be occasional or usual, using documents detailed in the KYC Checklist. Following applicant screening and background information check, along with review of business plan, source of funds, and expected levels of activity, an initial decision will be made with respect to the application status. This includes whether the client may be accepted, rejected, or whether more information may be required.

Clients should be made aware of the Company's explicit Policy that business transactions will not be conducted with applicants who fail to provide competent evidence of their activities and identity, but without derogating from the Company's legal and ethical obligations to report suspicious transactions.

Where initial verification fails to identify the applicant or give rise to suspicious suspicion that the information provided is false, additional verification measures should be undertaken to determine whether to proceed with the business transaction. Details of the additional verifications are to be recorded.

If, during the business relationship, there is any reason to doubt any of the following:

- the accuracy of the information relating to the customer's identity
- that the customer is the Beneficial Owner
- the intermediary's declaration of Beneficial Ownership,
- that there are any signs of unreported changes,

The Company shall then take further measures to verify the identity of the customer or the beneficial owner, as applicable. Such measures may include the following:

- referral of names and other identifying information to criminal investigating authorities; and
- review of disciplinary history and disclosure of past relevant sanctions.

The Customer Identification Programme must include procedures for responding to circumstances in which the Compliance Monitoring team cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe, among others, the following:

- When Emirates Gold should not do business with a client
- The terms under which a customer may conduct business transactions while the Company attempts to verify the customer's identity
- When Emirates Gold should file a Suspicious Activity/Transaction Report

It must also include procedures for providing customers adequate notice that the Company is requesting information to verify their identities.

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, the Company shall not proceed with a transaction for such Customer and shall flag the same as High-Risk. Such cases are marked for reporting to the Regulator through Suspicious Transaction Report (STR), and for increased monitoring.

### 12.03 Customer Onboarding

In general, the Company will have the following as its customers:

- Natural persons
- Legal persons, including individual members of corporates

### 12.03.01 Natural Persons and Individual Members of Corporate Customers

The Company shall obtain from all individual members of corporate customers, including shareholders, beneficial owners, directors, managers, authorised 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 the UAE nationals/residents)
- Physical Address (residential and business/home country and the UAE)
- Contact details
- Source of funds and wealth
- Declaration regarding Beneficial Ownership, that is, the person who has ultimate ownership
- Whether the customer is a Politically Exposed Person (PEP) or a Close Associate of a PEP

The above list is a summary of the information required.

As part of the process for identifying and verifying customers, and for authenticating the documents upon which the verification is based, the Company will include procedures for the certification of the customer identification and address documentation it obtains.

### 12.03.01 Legal Persons

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 the relevant Supervising Authority/Regulatory Agency shall be made.

The Company shall obtain from all corporate customers the following information:

- Incorporated name.
- Shareholders (To include 'active' and 'silent' or 'sleeping' partners).
- Ultimate beneficial owners (the Beneficial Owner shall be whoever person 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, 5% or more of the shares or 5% or more of the voting rights in the Legal Person).
- Managers (That person having day-to-day control of the company, if not a shareholder/partner).
- Authorised Signatories.
- Passport of all shareholders, Ultimate beneficial owners, Managers, and Signatories.
- National Identity Document of shareholders, Ultimate Beneficial Owners, Managers, Signatories (Emirates ID, if a customer is a resident/citizen of the UAE).
- Memorandum and Articles of Association.
- Power of Attorney (if applicable).
- Proof of physical address of the company.
- Contact details.
- Business activities (type and volume).
- Source of funds wealth (if applicable).

The above list is a summary of the information required.

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

The Company 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.

### 12.03 Risk Profiling

The Company uses the "Risk Profiling" forms to assess the ML/FT/PF risks the customers pose to the business, based on the information and documents obtained from the customer. 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.

Basis the risk score and the parameters observed, the Company classifies the customers as under:

- **High-Risk** customer, subject to Enhanced Due Diligence
- **Medium-Risk** customer, following the outcome of Enhanced Due Diligence measures
- **Low-Risk** customer, subject to Simplified/Standard Customer Due Diligence

### 12.04 KYC Process

The Company maintains clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher risk than average risk. Before accepting a client, KYC and due diligence procedures are followed by examining factors such as the customers' background, country of origin, public or high-profile position, business activities, or other risk indicators.

In case of Retail Business, the Company will carry on Simplified/Standard Due Diligence on all Low-risk clients and, in case any retail Business transaction is exceeding AED 55,000 (whether as a single transaction or Multiple Transactions), the Complete CDD process shall be followed.

KYC is to be carried out according to the procedures followed by the compliance team.

If the customer is unable to comply with the compliance team's requirements, the Company should:

- Not onboard the client, commence business relations, or perform the transaction.
- Terminate the business relationship.
- Consider filing a suspicious activity / transaction report in relation to the customer.

It is strictly forbidden for the Company to do business with shell companies. Shell companies shall mean an institution that has no physical presence in any country, no active business, and which merely exists on paper.

An integral part of the KYC process is the carrying out of customer screening and relative risk assessment. Screening ensures that a customer is not listed on the official sanctions lists issued by the 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.

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

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 discussions, visits, online searches, etc.,

and which is deemed to be relevant for 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.

### 12.05 High-Risk Customers and Enhanced Due Diligence ('EDD') Measures

The Company has a Policy to apply Enhanced Due Diligence measures in case of identified high-risk customers, where there are doubts about the appropriateness of the customer's ML/FT/PF risk classification. Further, in the following cases, the Company shall classify the customer risk category as "high" and shall perform the EDD measures:

- If the customer is suspected of being involved in any crime (financial, tax-related, or any other crime) or any other red flags or suspicious activities have been observed,
- The customer is a PEP or associated with a PEP.

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, and procedures will need to explain how the increased risks will be minimised. Should it be determined that a customer who fulfils the criteria for designation as high risk does not warrant EDD, the reasons for the decision and the way the risks are mitigated should still be fully documented and placed in the customer's file. In addition, any EDD procedures carried out during the approval process, together with the proposed procedures for future monitoring, should be fully documented and placed in the customer's file.

### 12.05 Politically Exposed Persons (PEPs)

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, who can be susceptible to bribery and corruption. For this Policy, the Company refers to the definition of PEPs as given under the AML/CFT Decision -

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

- *Direct Family Members (of the PEP, who are spouses, children, spouses of children, parents).*
- *Associates known to be close to the PEP, which include:*
  - *Individuals having joint ownership rights in a legal person or arrangement, or any other close Business Relationship with the PEP.*
  - *Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.*

Due to their position and influence, it is recognised that many PEPs are in positions that can be potentially abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption and bribery, as well as conducting activity relating to terrorist financing (TF) or find that their public position has been or is being unknowingly used for their benefit or benefit of others who may be involved in illegal activities such as corruption, bribery, fraud, etc.

Risk is increased considerably when a PEP is located in a high-risk country. The Company will ensure that each beneficial owner or controller is not a PEP by performing searches on official databases to

screen names against its database or by referring to publicly available information. The results of such verifications will be recorded within the customer KYC file.

If a PEP is identified, the Company will:

- Assign a rating of high risk to the customer,
- Complete Compliance Report highlighting the risk possessed with the PEP, ensuring that the Compliance team approves establishing a business with that customer,
- Conduct EDD and be vigilant in monitoring the business relationship,
- Ensure reasonable measures will be taken to establish source of wealth and source of funds,
- Track PEP relationships for the purposes of reporting and monitoring.

## 12.06 Sanctioned Individuals/Entities

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

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

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

As part of the CDD procedure, the Company has a Policy to undertake ongoing supervision and auditing of the transactions executed throughout the relationship with a customer to ensure consistency with the information and risk profiles of the customers.

## 12.07 Ongoing Monitoring of Business Relationship

As part of the CDD procedure, the Company has a Policy to undertake ongoing supervision and auditing of the transactions executed throughout the relationship with a customer to ensure consistency with the information and risk profiles of the customers.

### 12.06 Reliance on third parties for CDD

Though the Company has a Policy to internally perform the Customer Due Diligence procedures, however, in exceptional circumstances, the Company may rely on third parties to undertake CDD measures on our behalf. Such exceptional circumstances may include cases where the high-risk customer is located outside the UAE or in high-risk countries, and it is not feasible for the Company to undertake CDD directly.

## 12.08 Customer Acceptance Policy

To avoid any non-compliance or reputational damage to the Company, the following procedures and controls shall be adopted as part of the Customer Acceptance Policy:

- Accept only those customers whose identity is established by conducting due diligence appropriate to the risk profile of the customer.
- Where the customer is new, it can only be onboarded after ensuring that pre-account opening KYC documentation, Screening, and Risk Assessment procedures are conducted.
    - Documents as per standard norms to be collected.

- Identity verification of the customer is performed.
- In the case of customers categorised as "high" risk, the business relationship shall be established only upon completion of the Enhanced Due Diligence measures.
- Sign-off is obtained from the compliance team to onboard the customer.

The Company does not accept the establishment of a business relationship with entities or individuals of unknown identity or using fictitious or unreal names, or if there is reasonable doubt that the identification documents are falsified.

Further, the Company will not establish a business relationship with an individual or entity that:

- is a shell company itself,
- operates with virtual/shell banks,
- when any of the beneficiaries or the UBOs are unknown,
- where the associated ML/FT/PF risk exceeds the Company's risk appetite,
- customers associated with "high-risk" countries as mentioned under the FATF Blacklist.

### 12.09 Customer Exit Policy

The Company shall terminate an active business relationship if the customer's risk profile changes from "low" to "high" and the customer does not provide all the details and documents necessary for applying Enhanced Due Diligence measures for AML/CFT purposes.

Further, the Company shall off-board the existing customer under the following circumstances:

- when the customer gets associated with "high-risk" countries as mentioned under the FATF Blacklist,
- when the ML/FT/PF risks associated with the customer exceed the Company's risk appetite.

When the Company concludes that it cannot serve the customer anymore, it will treat the customer fairly and communicate in plain language.

As per the facts of the case, the Company would also consider filing the relevant report with the authorities:

- Suspicious Transaction Report
- Suspicious Activity Report
- Fund Freeze Report
- Partial Name Match Report
- High Risk Country Transaction Report
- High Risk Country Activity Report

In all cases, a log of exited/terminated/rejected cases would be maintained.

### 12.10 Cash Acceptance Policy

The Company shall accept the cash against its transactions only after checking the validity of the currency notes to identify any counterfeit bills and shall immediately reject the same and report the transaction to the FIU by filing a Suspicious Transaction Report.

Further, the Company shall report the transactions and the corresponding parties to the FIU by filing the Dealers in Precious Metals and Stones Report (DPMSR) upon receipt or payment of the funds equal to or exceeding AED 55,000 (including the linked payments and receipts).

## 13.0 Indicators of suspicious activities – red flags

Methods which criminals utilise to conduct money laundering, financing of terrorism, and financing of illegal organisations are constantly evolving, and as such, in many cases, there exist particularities within a given market or given type of trust and company service that may be beyond the scope of red flags identified within this Policy. Therefore, the following list of red-flag indicators of potentially suspicious transactions should by no means be treated as exhaustive.

It is noted that the presence of one or more of the indicators below does not necessarily mean that a transaction involves ML/FT/PF. However, it is an indication that enhanced due diligence, or further investigation may be required, so that an appropriate determination can be made by the Company's appointed Compliance Officer as to whether the transaction can be deemed suspicious or not.

A red flag should be raised with respect to trade practices in the following circumstances:

- Precious metals/stones originate from a country where there is limited production or no mines at all.
- Trade in large volumes conducted with countries which are not part of a specific precious metals and stones pipeline.
- An increase in the volume of the activity in a DPMS account despite a significant decrease in the industry-wide volume.
- Selling or buying precious metals and stones between two local companies through an intermediary located abroad (lack of business justification, uncertainty as to actual passage of goods between the companies).
- Volume of purchases and/or imports that grossly exceed the expected sales amount.
- A single bank account is used by multiple businesses.

A red flag should be raised with respect to the Business Relationship, or the Customer in the following circumstances if the customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, [Company Name] has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
  - their business activities and corporate history
  - the identity of the beneficial owner
  - their source of wealth/funds
  - why they are conducting their activities in a certain manner
  - who they are transacting with
  - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Is a designated person or organisation (i.e., is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.

- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for doing business with Emirates Gold.
- Is located a significant geographic distance away from the Company, with no logical rationale.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
- Makes unusual requests (including those related to secrecy) of Emirates Gold or its employees.
- Is prepared to pay substantially higher fees than usual, without a legitimate reason.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping of gold into ordinary-looking items) that could improperly disguise the nature of the PMS or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.
- Claims to be a legitimate DPMS but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others).
- Is registered under a name that does not indicate that the activity of the Company is related to PMS, or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for shortcuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.

- Requests payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or instalment arrangements, or payment in several different forms), or which involve third parties.
- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be processed exclusively or mainly through the use of cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

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.
- 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 authorised representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys).
- 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 tax 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).

**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 traveller's cheques, cashier's cheques, and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PMS. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Is divided 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.

## 14.0 Reporting of Suspicious Transactions/Activities

Emirates Gold shall establish a system for mandatory reporting of suspicious transactions in accordance with the UAE AML/CFT legislative and regulatory framework. All suspicious activities or transactions (SARs/STRs), along with any additional required information, must be reported to the FIU via the GOAML system. These reports must be filed within 5 working days after becoming aware of the suspicious transaction.

If any employee, director, officer, or personnel of Emirates Gold becomes aware that a client has engaged in predicate crimes, the matter must be promptly reported to the Compliance Officer. The Compliance Officer will then review the matter and, if sufficient evidence is available, escalate it to the Board of Directors to determine whether it should be reported to the FIU as Suspicious Activity. If there are reasonable grounds to suspect that the customer has engaged in unlawful activity, the Board of Directors will promptly evaluate whether there is sufficient evidence for such suspicion and, if necessary, report the case to the FIU, unless the Compliance Officer concludes otherwise.

Emirates Gold will maintain a register of all suspicious transactions brought to the attention of its Compliance Officer, including those not reported to the FIU. This register will include the date of the report, the individual who made the report, and sufficient details to identify the related documents. Additionally, Emirates Gold acknowledges that failing to report suspicious transactions, whether intentionally or through gross negligence, constitutes a federal crime. Individuals who fail to meet their legal obligations to report suspicions related to money laundering, terrorism financing, or illegal organisations may face fines, imprisonment, or both.

The company acknowledges the obligation to report suspicious transactions under the AML/CFT framework. To facilitate the identification of suspicious transactions, this Policy defines the concept of suspicious transactions to include any attempted or completed transactions where there are reasonable grounds to suspect that they involve proceeds of crime, money laundering, terrorism financing, or the financing of illegal organisations. This applies regardless of the amount or volume involved, and regardless of the timing. Transactions that may be suspicious include those where the proceeds are linked to criminal activity, even if committed outside the UAE, or those intended to fund illegal activities.

In line with this, Emirates Gold is committed to ensuring its staff receive adequate training to identify and report suspicious transactions, assess 'red flag' indicators, conduct internal investigations before reporting to the FIU, and understand the implications of failing to report suspicious transactions.

## 14.01 Types of Reporting on the goAML portal

### 14.01.01 Funds Freeze Report (FFR)

Reporting entities are supposed to file a Funds Freeze Report to report any freezing measure, prohibition to provide funds or services, and any attempted transactions related to confirmed matches. This report is raised when the reporting entity finds a full match of the customer's name with a name listed in the UAE LOCAL LIST or the UN CONSOLIDATED LIST.

### 14.01.02 Partial Name Match Report (PNMR)

This report is raised when the reporting entity cannot verify if the name of the customer is a full match to the name of a sanctioned person listed in the UAE LOCAL TERRORIST LIST or the UN CONSOLIDATED LIST.

### 14.01.03 Suspicious Transaction/Activity Reporting (STR/SAR)

Transactions that do not match the customer profile, high volumes of transactions being made in a short period of time, payment of high amounts by cash, cannot provide identification documents and source of funds;-are some examples of suspicious activities/transactions.

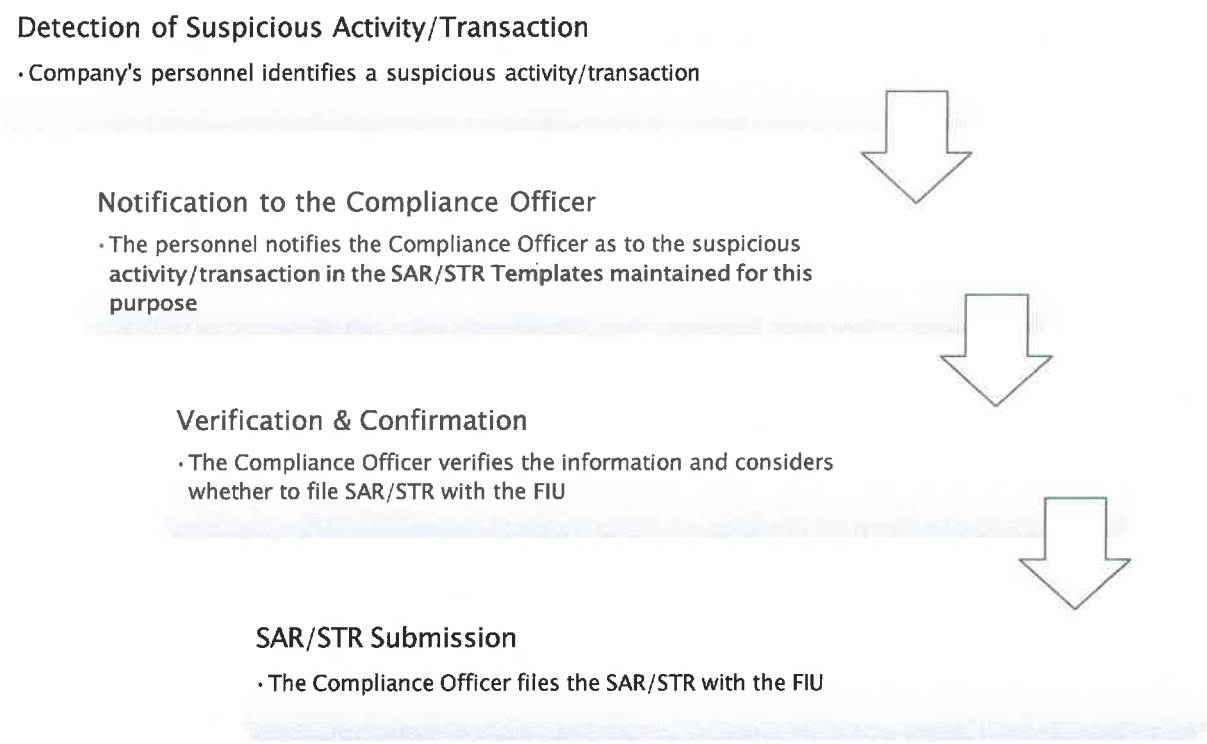
If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or a potential customer, a reporting entity suspects transactions or attempted

transactions related to money laundering, fraud or terrorist financing, then the entity should submit an STR/SAR to the FIU at the earliest.

File STR/SAR if a full/partial match of the customer's name is found on other international sanctions lists (e.g., OFAC, UKHMT, EU, etc)

If a reporting entity suspects or has reasonable grounds to suspect that funds/activity are the proceeds of a criminal activity, or are related to terrorist financing, it shall, as soon as possible but no later than 5 days report promptly its suspicions to the FIU.

Therefore, the overall workflow for the SAR/STR Submission Process is as follows:




### 14.01.04 High-Risk Countries Report / Activity (HRC/HRCA)

The obligation for reporting as well as putting on hold, is for cross-border transactions through banking or remittance channels. These transactions may include transactions destined to, originated from, or being routed through jurisdictions that are classified as a 'High-Risk Jurisdiction subject to a Call for Action' by FATF. Currently, this includes the Democratic People's Republic of Korea, Iran, and Myanmar.

Such reported transaction(s) 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.

### 14.01.05 Dealers in Precious Metals & Stones Report (DPMSR)

Dealers in Precious Metals and Precious Stones (DPMS) are identified under UAE law as Designated Non-Financial Business and Professions (DNFBPs) when they carry out a single transaction or several transactions, interrelated in appearance, whose value is equal to or greater than AED 55,000.

All international wire transfer Transactions with individuals/entities (B2C/B2B) equal or exceeding AED 55,000 need to be reported in DPMSR. Obtain and verify identification documents (ID or Passport) that need to be reported in DPMSR.

### 14.01.06 Tipping Off and Confidentiality

Tipping off a customer is an unauthorised act of disclosing information that:

May result in the customer, or a third party (other than FIU) knowing or suspecting that the customer is or may be the subject of:

- a suspicious transaction report; or

- an investigation relating to money laundering or terrorist financing; and

May prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorist financing.

Emirates Gold's directors, officers, and employees shall not warn customers that information relating to them has been or is in the process of being reported to the FIU, or communicate, directly or indirectly, such information to any person other than the FIU. Any violation of this confidentiality provision shall render them liable for criminal, civil, and administrative sanctions under the UAE AML/CFT law.

## 15.0 International Financial Sanctions

The United Arab Emirates is a member of several multinational and international organisations and governing bodies, including the United Nations. The Company is obliged to comply with the directives of the Competent Authorities of the State in relation to the agreements and conventions referred to above, including but not limited to Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions. Moreover, it should be noted that it is affected by unilateral international sanctions programmes and restrictive measures implemented by other countries and supranational blocs.

## 15.01 Targeted Financial Sanctions

Targeted Financial Sanctions are international sanctions rules established to comply with the United Nations Security Council resolutions under Chapter VII of the Charter of the United Nations. The UAE adheres to the decisions issued by the UN Security Council under that Chapter, as well as to the FATF recommendations concerning their implementation. The AML-CFT Law and its Implementing AML-CFT Decision provide that:

"Every natural or legal person shall immediately comply with the instructions issued by the Competent Authorities in the State concerning the implementation of the decisions issued by the UN Security Council under Chapter VII of the Charter of the United Nations regarding the prevention and suppression of terrorism and Terrorism Financing, and the prevention and suppression of the proliferation of Weapons of Mass Destruction and its financing, and any other related Decisions."

And further, that: "Imprisonment or a fine of no less than AED 5,000,000 million (five million dirhams) and no more than AED 100,000,000 (hundred million dirhams) shall be applied to any person who violates the instruction issued by the Competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions."

The AML-CFT Law and the AML-CFT Decision oblige DNFBPs to promptly apply directives issued by the Competent Authorities of the State for implementing the decisions issued by the UN Security Council under Chapter VII of the Charter of the United Nations.

Accordingly, the Company is committed to immediately freezing funds owned, controlled, or held, in whole or in part, directly or indirectly by any of the following:

1. An individual or organisation designated by the UN Security Council or any relevant Security Council Committee pursuant to any relevant Security Council resolutions.
2. An individual acting, directly or indirectly, on behalf of, or as directed, controlled, or dominated by, any person or organisation listed in the Sanctions List.

In all cases, the rights of bona fide third parties shall be considered when implementing any of the freezing procedures.

Once a customer becomes part of Sanctions List, the Company shall freeze funds (including assets in any form) of listed persons and organisations, which are in their possession or under their control, or which they receive for any reason (including as payment for products or services), even without receiving specific instructions from any Competent Authority to do so.

The Company is committed to:

- Maintaining a continuously up-to-date awareness of the persons and organisations listed in the relevant Sanctions Committees lists and comparing these on an ongoing basis with their customer databases.
- Ensuring, prior to entering into business relationships or conducting any transactions with natural or legal persons or legal arrangements, that such persons or organisations are not included in the relevant Sanctions List.
- Undertake regular and ongoing screening of the latest local terrorist list and UN Consolidated List. The company conducts screening in the following cases:
    - Upon any update to the Local Terrorist List or UN Consolidated List
    - Prior to onboarding new customers
    - Upon KYC Reviews or changes to customer information
- It is the Policy of the Company to perform screening of existing customers, suppliers, UBOs, parties to transactions, and agents.
- Freezing (or unfreezing when so instructed by the Competent Authorities) the Funds of listed persons or organisations, which the supervised institutions hold, have access to, or otherwise control.
- Immediately report to the Supervisory Authority when listed persons or organisations are identified and/or when the Funds of such persons or organisations are frozen.
- Immediately reporting to the relevant Supervisory Authority the details of any customers identified as listed persons or organisations regardless of whether they are past, current, or prospective customers; regardless of whether they maintain(ed) business relationships with such customers or interact(ed) with them only in the form of occasional or attempted transactions; and also regardless of whether they perform(ed) any transactions related to such persons or organisations, along with the action taken or proposed to be taken by the Company.
- Immediately reporting to the relevant Supervisory Authorities the details of any customers that are identified as potential matches with listed persons or organisations, when it cannot resolve the similarities (i.e., cannot either confirm the match as true or conclusively reject it as a false positive) based on the information available to and therefore have not frozen the Funds of such persons or organisations, or have not undertaken other procedures in compliance with the prohibition requirements prescribed in the relevant UN Security Council Resolutions. In such cases, the company shall avoid executing any transactions related to such persons or organisations, pending feedback or instructions from the relevant Supervisory Authorities.
- In the case of Suspicious Transactions (whether past, in-progress or attempted) involving listed persons or organisations, the company shall file the STRs with the FIU as per the normal procedures. At the same time, it shall report the details of the listed persons or organisations to the relevant Supervisory Authorities.

### 15.02 Other International Sanctions

In addition to TFS and related programmes of the United Nations, many other countries and supranational blocs also maintain international economic, trade, or travel sanctions programmes and restrictive measures of their own. Like the TFS regimes, these unilateral measures often require the freezing of funds or other assets of listed natural or legal persons and organisations. They may also require general or specific licences to conduct business or engage in transactions with persons or entities from certain countries.

If the Company engages in transactions in the currencies of those countries and supranational blocs, whether for their own account or on behalf of their customers and Business Relationships, they may be affected by such international financial sanctions regimes. Some of the major international financial sanctions programmes are those of:

#### 15.02.01 The United States of America

The United States (U.S.) maintains a significant number of economic, trade, and other sanctions programmes in accordance with its foreign Policy and national security objectives. Some of these programmes are comprehensive, affecting entire countries or jurisdictions, while others are selective, targeting specific governments, sectors, organisations, and/or persons.

Many of the U.S. sanctions programmes are administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"); however, some (e.g., certain trade licensing and travel restriction programmes) may be administered by other agencies of the U.S. government.

If the Company conducts business or transactions in U.S. dollars, then the clearing of U.S. dollar-denominated transactions through a US financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of OFAC sanctions programmes.

#### 15.02.02 The European Union

In the context of its Common Foreign and Security Policy (CFSP), the European Union maintains a number of economic, trade, and other sanctions programmes, or "restrictive measures." Such restrictive measures may be imposed against third countries, entities, or persons in line with the EU's CFSP objectives.

If the Company conducts business or transactions in euros, then the clearing of euro-denominated transactions through the EU financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of EU restrictive measures.

#### 15.02.03 The United Kingdom

In addition to the EU-wide restrictive measures that it has applied during its tenure as a member state of the European Union, the UK can also impose its own financial sanctions and restrictive measures under domestic legislation, including:

- Terrorist Asset-Freezing Act 2010 (TAFA 2010)
- Counter-Terrorism Act 2008 (CTA 2008)
- Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001)

If the Company conducts business or transactions in British pounds, then the clearing of British pound-denominated transactions through a UK financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of UK financial sanctions programmes.

## 16.0 Training and Awareness

Emirates Gold shall provide education and training for all its staff and personnel, including directors and officers, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and financing of terrorism and illegal organisation, and so that they are familiar the system in place for reporting and investigating suspicious matters.

The Company may, due to the scale and nature of its operations, look to appoint an independent Internal Auditor or Trainer who has relevant experience and expertise in the field of AML/CFT.

The Company shall, at least once a year, conduct refresher training to remind key staff and officers of their AML/CFT responsibilities and to make them aware of any changes in the laws, national and international, and rules relating to AML/CFT.

New employees will receive appropriate training within 30 days of their hire date. Training for all employees must include not only the legal elements of AML/CFT laws and regulations, but should also cover job-specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

To ensure the continued adherence to the Company's AML/CFT and KYC policies and procedures, all employees are required to confirm their awareness of the contents of this Compliance Policy by signing the acknowledgment form annually, or more frequently.

## 17.0 Record-keeping and Record Retention Policy

The following documents shall be considered as the Company's AML/CFT Documents:

- All clients' documentation as provided in the KYC checklist and/or correspondences, including the documents obtained during CDD and/or EDD.
- All documentation concerning a suspicious activity report concerning a client or applicant, together with any response or follow-up.
- Records of AML/CFT training sessions attended by the Company's staff, officers, and their affiliates, the dates, content, and attendees.
- Records of all AML/CFT decisions taken by the senior management.

The objective of keeping said records is to ensure that the Company can provide the basic information for the reconstruction of the transaction, at the request of the competent authorities.

Documents may be retained as originals or copies, or as scanned images onto pen drives, hard discs, online systems, cloud-based systems, etc., provided that such forms are admissible in the UAE Court of Law.

All records must be available for prompt and swift access by the relevant authorities when required. A request for such records by government authorities may be fulfilled within a reasonable time frame, not to exceed fifteen (15) business days.

The documents shall be maintained for a minimum period of **Five (5) years**, in accordance with the AML/CFT Law and Decision, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account,
- Completion of a casual transaction (in respect of a customer with whom no Business Relationship is established),
- Completion of an inspection of the records by the Supervisory Authorities,

- The issue date of a final judgment by the competent judicial authorities,
- Liquidation, dissolution, or other forms of termination of a legal person or arrangement.

**Abhijit Shah**
**CEO and Board Member**
**Emirates Gold DMCC**

## APPENDIX A - AML/CFT Legal and Regulatory Framework

### National Legislative and Regulatory Framework

As a committed member, the UAE contributes to global anti-money laundering efforts and combating financing of terrorism (AML/CFT) and strives to fully implement the standards set by the International Financial Action Task Force (FATF). In 2018, the UAE, with the extensive participation of all concerned authorities, conducted its first national risk assessment on money laundering and terrorist financing, identifying several high-risk areas. The following Laws and their Implementation Regulation have been issued to combat the threat of AML/CFT:

- Federal Decree Law No. (20) of 2018 is the foundational law for AML/CFT, establishing the framework and the Financial Intelligence Unit (FIU).
- Federal Decree-Law No. (10) of 2025 Concerning Combating Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons. It is the newest primary law, effective October 2025, replacing the 2018 law with enhanced penalties, broader scope, and new offences like proliferation financing.
- Federal Decree Law No. (26) of 2021 to amend certain provisions of Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
- Federal Decree-Law No. (7) of 2024 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. 5 of 2012 on Combating Cyber Crimes.
- Federal Law No. 7 of 2014 on Combating Terrorism Offences.
- 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 Decision No. (10) of 2019, the Executive Regulation for Law No. 20/2018, detailing implementation.
- Cabinet Resolution No. (134) Of 2025 Concerning the Implementing Regulation of Decree Law No. (10) Of 2025 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of the Proliferation of Weapons'.
- Cabinet Resolution No. (24) of 2022 Extends regulations to Virtual Asset Service Providers (VASPs).
- Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures as amended by Cabinet Decision No. (109) of 2023.
- 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.
- Cabinet Decision No. (132) of 2023 Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Decision No. (109) of 2023 Concerning the Regulation of Beneficial Owner Procedures.
- 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.

- Cabinet Resolution No. (71) of 2024 Regarding the Regulation of Violations and Administrative Penalties Imposed on Violators of Anti-Money Laundering Procedures.
- Regulation No. 1/2019 regarding declaration of currencies, negotiable bearer financial instruments, precious metals & precious stones in possession of travellers entering or leaving UAE (issued by the UAE Central Bank on 14/1/2019 pursuant to Article 8 of Federal Law No. 20/2018).
- Central Bank Board of Directors' Decision No. 59/4/219 regarding procedures for AML and CTF and Illicit organisations.
- Guidelines for Financial Institutions on anti-money laundering and combating the financing of terrorism and illegal organisations issued by the UAE Central Bank on 23/6/2019.
- Ministerial Decision No. (532) of 2019 regarding the establishment of the Anti-Money Laundering Department 2019
- 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.
- Ministerial Decision No. (68) of 2024 Regarding adherence to the Policy of Due Diligence Regulations for Responsible Sourcing of Gold.
- Circular No. 323 of 2019 regarding Ultimate Beneficial Ownership
- Circular No. (2) of 2023 Data Disclosure Notice for Dealers in Precious Metals and Stones.
- Circular No. 1 of 2024, which has updated the list of High-Risk Jurisdictions subject to Call for Action and the list of Jurisdictions under Increased Monitoring.
- Circular No. (3) of 2024 regarding updating the list of High-Risk Jurisdictions subject to Call for Action and the list of Jurisdictions under Increased Monitoring.

**International Legislative and Regulatory Framework**

Fighting against money laundering and financing of terrorism is critical for international security, the integrity of the financial system, and sustainable growth. In response to the threats posed by money laundering and terrorist activities, the international community has acted on many fronts, including the creation of various organisations that act as the international standard setters.

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

Among the major intergovernmental legislative bodies, and international and regional regulatory organisations, with which the government and the Competent Authorities of the UAE actively collaborate within the sphere of the international AML/CFT framework are:

- Financial Action Task Force (FATF)
- United Nations (UN) & UN Security Council (UNSC) Committees
- United Nations Office on Drugs and Crime (UNODC)
- Egmont Group of Financial Intelligence Units (FIUs)
- International Monetary Fund (IMF)
- World Bank
- Organisation for Economic Co-operation and Development (OECD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Secretariat General of the Gulf Cooperation Council (GCC)
- Arab Monetary Fund (AMF)