AML/CFT Policy

Clique Gold LLC

REVISION HISTORY

Document Name: AML/CFT Policy
Created: 11/01/2024
Updated:
Controller: Compliance Officer
Owner: Compliance Officer
Classification: Company Confidential

All documents within **Clique Gold LLC** are classified in the following way. **PUBLIC** documents are intended for anyone, and **COMPANY CONFIDENTIAL** documents are to be kept confidential within the Company and used for normal business activities by the general office population, **HIGHLY CONFIDENTIAL** documents are to be kept confidential to restricted individuals within the Company.

Date	Version	Comments/Summary of change
11/01/2024	Ver0001.000	The first draft
		-

Table of Contents

1.0 INTRODUCTION

In response to the international community's growing concern about the problem of money laundering and the financing of terrorism, UAE and many countries around the world are enacting or strengthening their laws on the subject. Along with the society and the authorities of various countries, **Clique Gold LLC (hereinafter "the Company")** recognizes the importance of the fight against money laundering and terrorism financing since it impacts fundamental aspects of social life.

The Company is engaged in the trading of precious metals, stones, and jewellery.

The Company understands that the best way to fulfil this commitment is to establish effective internal policies and procedures that are conducive to:

1. Carrying out the activities and services provided in accordance with strict ethical standards and current regulations around Anti-Money Laundering and Combating Financing of Terrorism,
2. The implementation of codes of conduct and monitoring and reporting systems to prevent the Company from being used as a means for money laundering and terrorism financing,
3. Ensuring that all the employees of the Company observe "Know Your Customer" policies and procedures,
4. Strict compliance with applicable anti-money laundering and terrorism financing laws, as well as with the recommendations issued by the International Financial Action Task Force and international and UAE authorities.

As a result, the Company's management and employees must be vigilant for any suspicious activity and report it immediately to the established internal bodies, in accordance with specified policies and procedures, so that they may, in turn, notify the relevant authorities.

Only through the commitment of all Company executives and employees will it be possible to guarantee that the products being marketed, and the services being provided are not being used for money laundering or terrorism financing purposes.

Adherence to this policy is fundamental to ensuring that Company complies fully with anti-money laundering and terrorism financing legislation. The Company should therefore be actively involved in the policy's implementation and development.

This policy establishes minimum standards that a Company should observe and is defined according to the UAE AML/CFT legislation:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, *as amended* (the "AML-CFT Law" or "the Law"),
- Implementing regulation, Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, *as amended* (the "AML-CFT Decision" or "the Cabinet Decision"),
- Federal Law No. (7) of 2014 On Combating Terrorism Offences,
- 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,
- AML/CFT Guidelines for Designated Non-Financial Businesses and Professions,
- UAE Ministry of Economy's Supplemental Guidance for Dealers in Precious Metals and Stones.

The relevant reference has also been taken from the Financial Action Task Force (FATF) and the Middle East and North Africa Financial Action Task Force (MENAFATF) recommendations.

Compliance with the contents of this AML/CFT Policy is required by all Company executives and employees. Non-compliance with the criteria and guidelines contained in this Manual will lead to the corresponding responsibilities and sanctions. The contents of the Manual will prevail over other internal regulations that could conflict with these, except for those that establish stricter conduct codes and/or measures.

2.0 THE IDENTIFICATION AND ASSESSMENT OF ML/FT & PF RISKS

As one of the DNFBPs, the Company is required by Federal Decree-Law No. (20) of 2018, Article 16.1(a) and Cabinet Decision No. (10) of 2019, section 2, Article (4.1) to identify and assess ML/FT risks. Further, Federal Law No. 13 of 2007, Federal Decree-Law No. 12 of 2008, Federal Decree-Law No. 43 of 2021, Cabinet Decision No. (10) of 2019, Cabinet Resolution No. 50 for 2020, Federal Decree Law No. (20) of 2018 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.

2.01 Risk-Based Approach

The Company adopts a risk-based approach for the identification of ML/FT and Proliferation Financing (PF) risks. The objective is to identify, assess, and understand risks in accordance with the nature and size of the Company and be 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.

In this regard, the Company has a Policy to perform Enterprise-Wide Risk Assessment from AML/CFT and PF perspective to understand the risks the Company is exposed to and define the adequate mitigation measures corresponding to the risk and its assessed impact.

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

2.02 The Standard ML Model and Generic ML/FT Risks

To precisely understand and assess the MF/FT risk to which the Company is exposed, it is important that all the employees and executives of the Company are aware of the source of such risk. For this, the standard money laundering model is described as consisting of three phases, summarized hereunder:

- **Placement**
  In this phase, criminals attempt to introduce funds or the proceeds of crime into the financial system using various techniques or typologies. Once the funds or proceeds are introduced or placed into the financial system, they proceed to the next phase of the process.

- **Layering**
  In this phase, criminals attempt to disguise the illicit nature of the funds or proceeds of crime by engaging in transactions or layers of transactions that aim to conceal their origin.

- **Integration**
  In this phase, criminals attempt to return or integrate their "laundered" funds or the proceeds of crime back into the economy or to use them to commit new criminal offenses through transactions or activities that appear to be legitimate.

The terrorists and criminals involved in these acts attempt to exploit situations, and factors favour anonymity and complexity to obscure and conceal the illicit source of the funds, the illicit destination or purpose for which they are intended, or both.

2.03 ML/FT Typologies

As the methods used by criminals for money laundering or the financing of terrorism / illegal organizations are continually evolving, it is therefore critical for the Company to ensure that its personnel is kept up to date on the latest ML/FT trends and typologies to combat the same. Accordingly, it is the policy of the Company to carry out a regular review of ML/FT trends and typologies in its compliance training program and risk identification and assessment procedures.

Some examples of ML/FT typologies:

- Use of precious metals and stones as an alternative to currency.
- Precious metals and stones as stored value instruments/means to realize the proceeds of crime, diamonds and gold are an international commodity, easily traded, transferrable across borders, and able to retain (or even appreciate in) value over relatively long periods of time.
- Laundering illegal precious metals and stones and/or the use of precious metals and stones to launder the proceeds of crime.

- Trade-based money laundering, such as over-invoicing, under-invoicing, or fraudulent invoicing, forgery and falsification of documentation, virtual trading, and others.
- Physical smuggling of precious metals and stones, due to their high value-to-weight ratio.
- Transfers through traditional payment/remittance systems.
- Transfers through alternative or non-traditional payment/remittance systems.
- Physical transport, or "muling", of cash and other stored-value systems (e.g., prepaid cards, traveler's cheques, bank drafts, bills of exchange, or other negotiable bearer instruments).
- Use of business structures and third-party intermediaries.
- Customs, or value-added tax fraud.

2.04 Risk Factors

To implement a risk-based approach to assessing and mitigating risks, it is crucial to identify risk factors. The Company identifies and categorizes 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.

The Company considers the following parameters while assessing the ML/FT/PF risks, in line with the factors suggested by the NRA, Supervisory Authorities, etc.:

a. Customers or Business Relationship Specific Risk
b. Geographic Risk
c. Product, Service, Transaction Related Risk
d. Channel-Related Risk
e. Technology-Related Risk
f. Proliferation Financing Risk
g. Tax Crime-Related Risk

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

2.05 Risk Assessment and Risk Assessment Operations

The AML/CFT Law 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."

Furthermore, the AML-CFT Decision charges supervised institutions with: "...Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."

The Company understands its responsibility to assess continuously, document, and update its assessment based on the various risk factors identified above, including the factors involving time and trends.

Accordingly, the Company documents its risk assessment operations, analysis, and supporting data commensurate with the nature and size of its business.

3.0 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 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 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 MF/FT risk category whenever the circumstance change which arises a doubt about the accuracy or appropriateness of the originally designated ML/FT risk category.

3.01 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.

3.01.01 Business Relationship

For 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.

3.01.02 Occasional Transaction

The Company has the policy to carry out due diligence of all customers even if they enter transactions occasionally.

3.01.03 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 in a different way. We have identified such exceptional scenarios and adequate action in such situations as under:

- When the ML/FT 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 in an escrow account.
- 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.

3.02 Identity Verification

The Company has a policy to identify the customers, suppliers, beneficial owners, beneficiaries, or controlling persons and verify their identity based on documents and independent sources.

3.03 Risk Profiling

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

Basis the risk score and the parameters observed, the Company has a policy to classify the customers as under:

- **High-risk** customer, subject to Enhanced Due Diligence
- **Medium-risk** customer, subject to Standard Customer Due Diligence
- **Low-risk** customer, subject to Standard Customer Due Diligence

- **Unacceptable**, wherein the Company shall not establish any business relationship with the customer.

3.04 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 appropriateness of customer's ML/FT risk classification or cases where there are red flags of potentially unusual or suspicious activity. 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 tax-related crime or any other crime,
- Customer is a PEP or associated to PEP.

For the purpose of this Policy, the Company refers to the definition of PEPs as given under 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 organization or any prominent function within such an organization; and the definition also includes the following

- *Direct Family Members (of the PEP, who are spouses, children, spouses of children, and parents).*
- *Associates known to be close to the PEP, which includes*:
  - *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.*

3.05 Ongoing Monitoring of Business Relationships

As part of the CDD procedure, the Company has the 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.

3.06 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 the 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.

3.07 Customer Acceptance Policy

The Company's Customer Acceptance Policy (CAP) is an important policy in determining the basis on which the Company enters relationships with its customers. An inadequate CAP or the inadequate implementation of the CAP can expose the Company to serious compliance, legal and reputational risks.

3.08 Customer Exit Policy

While deciding to exit a customer, the Company will assess the risks associated with a customer on an objective and non-discriminatory basis. The Company has the policy to consider the laws and regulations in the jurisdiction in which it operates. The reason to exit a customer could arise from several factors, including the money laundering and terrorist financing risks associated with a customer, strategic business decisions, customer viability, or overall costs.

3.09 Cash Acceptance Policy

The Company has a policy of not accepting cash payments against the supply of precious metals and stones.

4.0 REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

We understand the obligation imposed on the Company to report suspicious transactions to the Financial Intelligence Unit under AML/CFT Decision.

For ease in identifying whether a transaction can be construed as a "suspicious transaction", the said concept has been included as part of this policy **(for transactions in-progress or proposed or concluded transactions and irrespective of the amount or volume involved)**, as under:

Any transaction attempted transaction or funds which the employees of the Company have reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing—any of the following:

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

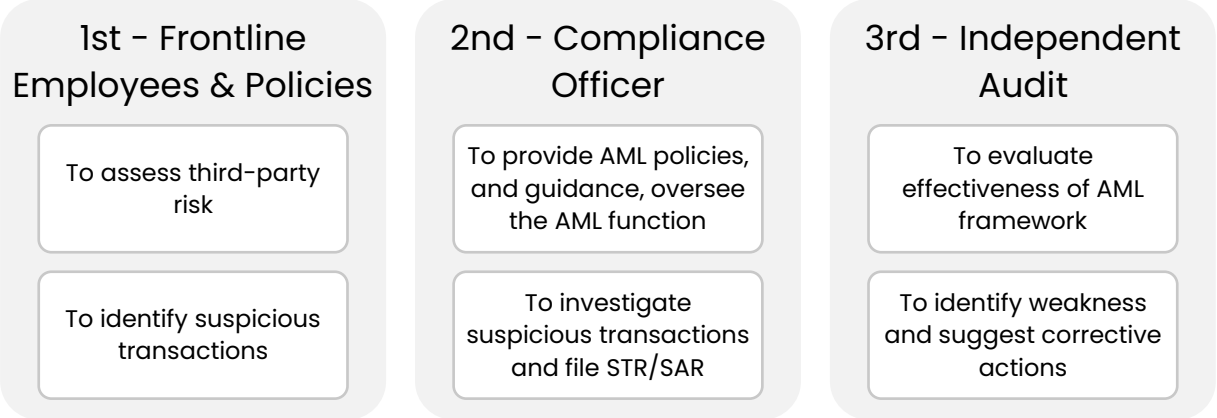
The Company understands its responsibility and is committed to ensuring adequate training programs for its staff with respect to:

- Identification and reporting of suspicious transactions,
- Appropriate assessment of the 'red flag' indicators,
- Adequate internal investigation by the Compliance Officer before reporting the suspicious transaction to FIU,
- Understand the implications for the employee and Company in case of failure to report the suspicious transaction.

5.0 AML/CFT GOVERNANCE

5.01 Three lines of defense

The Company shall follow the 3 lines of defence mechanism to safeguard its business against ML/FT/PF risk, as prescribed below:



5.02 AML/CFT Governance Elements

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

5.02.01 Appointment of AML/CFT Compliance Officer

For better adherence and compliance with the AML/CFT regulation and oversight of the effective implementation of this Policy, the Company appointed **Mr. Nagarajan Mahalingam** as the AML/CFT Compliance Officer ('CO') of the Company. The CO shall avoid the conflict of interest between the day-to-day routine of the Company related to supply of goods or services and customer business relationship management and AML compliance.

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

- **AML/CFT Program Management:** The CO would be responsible for ensuring the quality, strength, and effectiveness of the Company's AML/CFT program. 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 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.

5.02.02 Staff Screening and Training

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

The CO shall continually monitor the training needs.

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

5.02.03 Group Oversight

The Company does not have any branch/es.

5.02.04 Independent Audit Function

The Company has a Policy to implement an independent AML Audit function to test the effectiveness and adequacy of our internal policies, controls, and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations.

5.02.05 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 with regard to 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, duly approved by the Supervisory Authority,
- 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 to the relevant Supervisory Authority,

- 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 and Terrorism Financing.

5.03 Maintenance of AML/CFT Registers

For effective collation of data around AML/CFT, the Compliance Officer shall ensure maintenance of the adequate registers.

6.0 RECORD-KEEPING

The Company is committed to maintaining the records in an organized fashion to permit data analysis and the tracking of financial transactions and to make the records available to the Competent Authorities immediately upon request. 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.

7.0 INTERNATIONAL FINANCIAL SANCTIONS

The United Arab Emirates is a member of several multinational and international organizations 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 programs and restrictive measures implemented by other countries and supranational blocs.

7.01 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 50,000 (fifty thousand dirhams) and no more than AED 5,000,000 (five 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 organization 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 organization 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 organizations, 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 organizations 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 organizations 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
    - Before processing any transaction
- 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 organizations, which the supervised institutions hold, have access to, or otherwise control.
- Immediately report to the Supervisory Authority when listed persons or organizations are identified and/or when the Funds of such persons or organizations are frozen.
- Immediately reporting to the relevant Supervisory Authority the details of any customers identified as listed persons or organizations 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 organizations, 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 organizations, 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 organizations, 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 organizations, 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 organizations, 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 organizations to the relevant Supervisory Authorities.

7.02 Other International Sanctions

In addition to TFS and related programs of the United Nations, many other countries and supranational blocs also maintain international economic, trade, or travel sanctions programs 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 organizations. 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, may be affected by such international financial sanctions regimes. Some of the major international financial sanctions programs are those of:

7.02.01 The United States of America

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

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

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

7.02.02 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 programs, 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 EU financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of EU restrictive measures.

7.02.03 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 also can 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 programs.

7.03 Sanction Screening, Alert Management, Reporting

In order to fulfil their obligation to comply with the provisions of Cabinet Decision No. (74) of 2020, as well as with the directives of the relevant Competent Authorities and Supervisory Authorities in regard to TFS and other decisions issued by the UN Security Council, and to manage their exposure to the risks associated with unilateral international financial sanctions programs and restrictive measures implemented by other countries, the Company shall take steps to ensure that it has adequate internal policies, procedures, and controls in place, commensurate with the nature and size of the businesses

AML/CFT Policy Approved By:

Signature:

Name:

Designation:

GLOSSARY

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 United Arab Emirates.
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 organizations.
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.
Crime	Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organizations.
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.
Customer	Anyone who performs or attempts to perform any of the acts defined in Article 2 and 3 of the present Decision with any Designated Non-financial business or profession.

Term	Definition
Decree-Law (or "AML-CFT Law")	Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations.
AML-CFT Decision (or "Cabinet Decision")	Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Designated Non-financial Businesses and Professions (DNFBPs)	Anyone who conducts one or several of the commercial or professional activities defined in the Executive Regulation of this Decree-Law.
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 organizations 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 Organizations	Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or members.
Financing of Terrorism	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014 on combating terrorism offences.
FIU	Financial Intelligence Unit.
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

Term	Definition
	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 Organizations	Organizations whose establishment is criminalized, or which exercise a criminalized activity.
Law Enforcement Authorities	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidences on the crimes, including AML/CFT crimes and financing illegal organizations
Legal Arrangement	A relationship established by means of a contract between two or more parties, including but not limited to Trust funds or other similar arrangements.
Local 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 co-operation and co-ordination 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 Organizations (NPOs)	Any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit Legal Arrangements for the purpose of collecting, receiving, or

Term	Definition
	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 organization or any prominent function within such an organization; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which 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 favor of the PEP.
Predicate Offense	Any act constituting an offense or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.
Proceeds	Funds generated directly or indirectly from the commitment of any felony or misdemeanor including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
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 organizations, 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 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) which fall under the scope of Federal Decree-Law No. (20) of 2018 on Facing Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, and of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of

Term	Definition
	Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
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 organizations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations.
Suspicious Transactions	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any felony or misdemeanor or related to the Financing of Terrorism or of illegal organizations, 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 for 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 to 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 nature or legal person.

USEFUL LINKS

- UAE goAML Registration
- UNSC Sanctions List
- UAE Local Terrorist List
- Download Guidelines for Designated Non-Financial Businesses and Professions
- Download Supplemental Guidance for Dealers in Precious Metals and Stones
- FATF
- Egmont Group
- MENAFATF
- United Nations Office on Drugs & Crime – Global Programme Against Money Laundering
- Wolfsberg Group
- UN press releases