



AML/CFT POLICIES & PROCEDURES

CONTENTS

1. PURPOSE
2. SCOPE
3. OBJECTIVES
4. COMPANY'S COMMITMENT
5. OBLIGATIONS FOR DPMS
6. MONEY LAUNDERING AND TERRORISM FINANCING
7. COMPLIANCE OFFICER – DESIGNATION & DUTIES
8. DUE DILIGENCE
9. CUSTOMER ACCEPTANCE POLICY
10. CASH ACCEPTANCE PROCEDURES
11. MAINTENANCE OF RECORDS & THEIR RETENTION
12. MONITORING SUSPICIOUS ACTIVITY
13. ONGOING MONITORING
14. REPORTING TO FINANCIAL INTELLIGENCE UNIT
15. REPORTING PROCEDURES TO SENIOR MANAGEMENT
16. INTERNAL AUDIT
17. INDEPENDENT / EXTERNAL AUDIT
18. EMPLOYEES TRAINING
19. CONFIDENTIAL REPORTING OF AML NON-COMPLIANCE
20. REVIEW
21. COMMUNICATION
22. FINES & PENALTIES
23. DISCLAIMER
24. ANNEXURE

PURPOSE

This policy has been formed in the light of FIU Regulations, Circulars & Notifications on Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT).

In pursuance of the :

- Federal Decree-Law No. (20) of 2018,

-Cabinet Decision No. (10) of 2019,

-Cabinet Decision No. (58) of 2020, and related circulars & notifications by the Ministry of Economy (MOE);

The policy of the company is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or terrorist financing. Money Laundering (ML) is generally understood as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds or assets so that they appear to have been derived from legitimate origins or constitute legitimate assets.

The purpose of this policy is to establish the general framework within **AL NASER INTERNATIONAL** for the fight against money laundering (ML) and financing of terrorism (FT).

This Policy sets out those provisions, procedures, and controls as enacted by **AL NASER INTERNATIONAL** concerning Anti-Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT").

The rationale behind the Policy is crystal clear; **AL NASER INTERNATIONAL** will only accept those business associates/ clients/ customers; whose sources of precious metals or funds can be reasonably established as legitimate; and that do not pose any risk (actual or potential) to **AL NASER INTERNATIONAL**'s reputation.

Considering the foregoing, **AL NASER INTERNATIONAL** will not tolerate any involvement in illegal activities or unauthorized activities by its staff, business associates/ clients/ customers.

Initiatives by **AL NASER INTERNATIONAL**

The basic purpose of the AML Policy is to establish a system for **AL NASER INTERNATIONAL** to participate in the international efforts against ML and to duly comply with the guidelines as detailed in the various circulars & notifications of FIU, and other legal provisions and to ensure that **AL NASER INTERNATIONAL** is not used as a vehicle for ML. The AML framework of **AL NASER INTERNATIONAL** would meet the extant regulatory requirements.

The Company is registered on the goAML portal.

We confirm that we are observing and complying with domestic and international laws, rules and regulations, including those governing the illicit trade in precious metals and the United Nation Security Council (UNSC) sanctions.

SCOPE

This AML Policy establishes the standards of AML compliance and is applicable to all activities of **AL NASER INTERNATIONAL**.

The UAE, cognizant of the need for regulatory legislation, has enacted numerous laws at federal level to prevent and criminalize money laundering and financing of terrorism.

AL NASER INTERNATIONAL is obligated to establish a set of policies & procedures to ensure that neither its clients nor their affiliates facilitates money laundering and/or the financing of terrorist activities.

References provides the list of these laws.

OBJECTIVES

- i. To establish a framework for adopting appropriate AML Procedures and controls in the operations / Business processes of **AL NASER INTERNATIONAL**.
- ii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- iii. To comply with applicable laws and regulatory guidelines.
- iv. To take necessary steps to ensure that the concerned staff is adequately trained and KYC/AML procedures are implemented.
- v. To assist law enforcement agencies in their effort to investigate and track money launderers.

COMPANY'S COMMITMENT

AL NASER INTERNATIONAL is a company registered under HAMRIYAH FREE ZONE AUTHORITY (HFZA), UAE. The company deals in imports, exports, trading of non-manufactured precious metals. The Company is covered under the United Arab Emirates Federal Decree Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations (the "AML/CFT Law").

As per this law, the company is obligated to establish a set of policies and procedures to ensure that it does not participate or facilitate money laundering and/or the financing of terrorists or criminal activities.

AL NASER INTERNATIONAL is strictly committed to adhere to the policies, rules, regulations and guidance provided by the Government of UAE.

AL NASER INTERNATIONAL continue to train its staff on the vulnerability of the DPMS sector and based on the regulations on the anti-money laundering and combating financing of terrorism & criminal activities with a specific emphasis on the KYC (Know Your Customer) and Due Diligence Principle. Our staff are also encouraged to participate in the various seminars organized by the various authorities and local bodies such as Dubai Gold & Jewellery Group.

We commit to rejecting or immediately suspending and discounting engagement with suppliers or customers where we identify a reasonable risk that they are sourcing (or are linked) to parties committing any of the crimes described above.

We will not tolerate any direct or indirect support to non-state armed groups or their affiliated who:

- i. Illegally control mine sites, transportation routes or other points in the supply chains.
- ii. Illegally tax or extort money or minerals at points in the supply chain, such as mining sites, or points where minerals are traded or exported

The issuance of this Policy together with the implementation, operation, and enforcement of the procedures and controls therein, reflects **AL NASER INTERNATIONAL's** commitment in this regard.

To combat money laundering and/or the financing of terrorism, **AL NASER INTERNATIONAL** shall co-operate with UAE and international government agencies, and recognized law enforcement agencies.

INTERNATIONAL

OBLIGATIONS FOR DEALERS IN PRECIOUS METAL & STONES (DPMS)

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 (the AML/CFT decision), identifies the dealers in precious metals & stones (DPMS) as Designated Non-financial Business & Professions (DNFBPs), when they engage in carrying out any single monetary transaction, or several transactions which appear to be interrelated, whose value is equal to or greater than AED 55,000; and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates (UAE).

The principal obligations of **AL NASER INTERNATIONAL** under the AML-CFT Law, AML-CFT Decision and Related Resolutions relate to the following categories of actions:

- 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 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;
- 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 reporting to the Supervisory Authorities when listed persons or organizations are identified and/or when the Funds of such persons or organizations are frozen, as well as in other specific situations stated in AML-CFT Law.
-

MONEY LAUNDERING AND TERRORISM FINANCING

Money Laundering means:

Money laundering is the practice of making money that was gained through criminal means, such as smuggling weapons drugs etc., look as if it came from a legitimate business activity. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

It includes any act mentioned in **Clause (1) of Article (2)** of Federal Law no. (20) of 2018 of AML/CFT law, UAE.

Terrorism financing means:

The provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations.

Here, provisions of Federal Law no. (7) of 2014 regarding terrorists act may apply.

Stages of Money Laundering

i. Placement

This is the first stage of money laundering is known as 'placement', whereby 'dirty' money is placed into the legal, financial systems. After getting hold of illegally acquired funds through theft, bribery and corruption, financial criminals move the cash from its source. This is where the criminal money is 'washed' and disguised by being placed into a legitimate financial system,

Examples of Placement

1. Blending of funds.
2. Invoice fraud.
3. Through 'smurfing'.
4. Offshore Accounts.
5. Carrying Small Sums of Cash Abroad.
6. Through Aborted Transactions.

ii. Layering

The second stage in the money laundering process is referred to as 'layering'. This is a complex web of transactions to move money into the financial system, usually via offshore techniques. Once the funds have been placed into the financial system, the criminals make it difficult for authorities to detect laundering activity. They do this by obscuring the audit trail through the strategic layering of financial transactions and fraudulent bookkeeping.

iii. Integration

The third of the stages of money laundering is 'integration'. The 'dirty' money is now absorbed into the economy, for instance via real estate. Once the 'dirty' money has been placed and layered, the funds will be integrated back into the legitimate financial system as 'legal' tender.

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

COMPLIANCE OFFICER – DESIGNATION & DUTIES

The company has designated a Compliance Officer for due compliance of its AML measures. She will act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions.

The compliance officer appointed, have the appropriate competencies and experience and under his/her own responsibility, shall perform the following tasks:

- *Detect Transactions relating to any Crime.*
- *Review, scrutinize and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.*
- *Review the internal rules and procedures relating to combating the Crime and their consistency with the Decretal-Law and the present Decision, assess the extent to which the institution is committed to the application of these rules and procedures, propose what is needed to update and develop these rules and procedures, prepare and submit semi-annual reports on these points to senior management, and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions.*
- *Prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organizations, and the means to combat them.*
- *Collaborate with the Supervisory Authority and FIU, provide them with all requested data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties.*

Powers and Responsibilities of Compliance Officer

- She is expected and empowered to act independently in carrying out the responsibilities vested in him.
- She should ensure that the entity follows a risk-based policy which is in line with guidelines by the Ministry of Economy.
- She is expected to ensure that KYC of all customers/suppliers is done and is updated time to time.
- She is in-charge of scrutinizing and reporting STRs, also for detection of transactions related to the crimes of ML/FT for reporting suspicions to the FILJ.
- She should ensure the quality, strength and effectiveness of the AML/CFT programme. He also ensures that all transactions and functions of the company are complying with and in conformity with the directives / circulars issued by the authorities from time to time.
- She should inform and report to senior management on the level of compliance and report it to the relevant Supervisory Authority.
- She is responsible for helping to establish and working with senior management and other internal and external stakeholders to ensure that the Company's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat

posed by ML/FT. They should also be updated with the guidelines issued by Ministry of Economy, Central Bank/FIU any other competent authority time to time.

DUE DILIGENCE

- The Company has undertaken required CDD measures to verify the identity of the Customer and the Beneficial Owner before or during the establishment of the business relationship or before executing a transaction for a Customer with whom there is no business relationship.
- And in the cases where there is a low crime risk, it will take necessary measures to complete verification of Customer identity after establishment of the business relationship, under the following conditions:
 - (a) The verification will be conducted in a timely manner as of the commencement of business relationship or the implementation of the transaction.
 - (b) The delay is necessary in order not to obstruct the natural course of business.
 - (c) The implementation of appropriate and effective measures to control the risks of the Crime.
- The Company has taken requisite measures to manage the risks in regard to the circumstances where Customers are able to benefit from the business relationship prior to completion of the verification process.

Customer Due Diligence (CDD) Measures

- CDD will be conducted for every client. CDD measures are comprised of several components, in keeping with the customer's ML/FT risk classification and the specific risk indicators that are identified.
- Generally, these components include, but are not limited to, the following categories:
 - Identification of the customer, Beneficial Owners, beneficiaries, and controlling persons; and the verification of their identity based on documents, data or information.
 - Screening of the customer, Beneficial Owners, beneficiaries, and controlling persons, to screen for the applicability of targeted or other international financial sanctions,
 - Obtaining an understanding of the intended purpose and nature of the Business Relationship, its ownership and control structure.
 - Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behaviour.
 - Scrutinizing transactions undertaken throughout the course of that relationship to ensure consistency.
 - Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant.

Enhanced Due Diligence (EDD) Measures

AL NASER INTERNATIONAL will enhance the measures regarding customers identified as high-risk, including the specific categories of customers as provided for in the relevant articles of the AML-CFT Decision, such as politically exposed persons (PEPS) customers associated with high-risk countries.

AL NASER INTERNATIONAL will intensify their measures, specifically by obtaining further evidence and supporting documentation. **AL NASER INTERNATIONAL** will ask for additional information and evidence from high-risk customers such as:

- Source of funds (revenue) and source of wealth;
- Identifying information on individuals with control over the customer (legal person or arrangement), such as signatories or guarantors;
- Occupation or type of business; d Financial statements;
- Banking references;
- Domicile;

Description of the customer's primary trade area and whether international transactions are expected to be routine; h Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and Explanations for changes in business activity.

Requirements for High-Risk Countries

AL NASER INTERNATIONAL shall consider the following measures:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources regarding the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;
- More detailed inquiry and evaluation of reasonableness regarding the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- Increased investigation to ascertain whether the customers or related persons (Beneficial Owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPS;
- Increased supervision of the Business Relationship, including the requirement for higher levels of internal reporting and management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information.

Simplified Due Diligence (SDD) Measures

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

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

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

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

1. Identified low-risk customers
2. Listed Companies

CUSTOMER ACCEPTANCE POLICY

- **AL NASER INTERNATIONAL** will ensure that customers and suppliers accepted by the company meet the criteria set for AML/CFT compliance under UAE law.
- The company will follow the following procedures for customer acceptance:
 - To perform CDD on all new customers, including but not limited to collecting, checking, and verifying the following:
 - Commercial / Trade / Operating License.
 - Certificate of Incorporation.
 - Memorandum and Articles of Association.
 - Share Certificate.
 - Registry Extract.
 - VAT Certificate / TAX Certificate.
 - Proof of Address.
 - Identification of all beneficial owners holding 25% or more of the shares.
 - Collecting information on the nature and purpose of the business relationship.
 - To categorize customers as low, medium, or high risk based on factors such as:
 - Nature of the business (Products and Services).
 - Customers / Suppliers.
 - Geographic location.
 - Transaction patterns.
 - Delivery channels.
 - Other risk factors.
 - The compliance officer to apply appropriate levels of due diligence based on the risk category.
 - To perform Enhance Due Diligence (EDD) for high-risk customers (e.g., PEPs or those from high-risk jurisdictions), and to collect:
 - Detailed source of funds.
 - Information on the customer's business or employment.
 - Senior management approval before establishing the relationship.
 - The compliance officer should conduct more frequent reviews and transaction monitoring.

- The Senior management of **Al Naser International** must review and approve the onboarding of high-risk customers and to support, the compliance officer should document the approval process, including the rationale for acceptance.
- The compliance officer will continuously monitor the customer transactions for any inconsistencies or suspicious activity.
- The compliance officer will update customer risk profiles periodically and whenever there are significant changes in the customer's circumstances.

CUSTOMER EXIT POLICY

To manage the termination of business relationships of **AL NASER INTERNATIONAL** in a manner that complies with AML/CFT regulations in the UAE the following procedures will be followed:

- Criteria for Exit:
 - Define specific criteria for exiting a customer relationship, such as:
 - Non-compliance with AML/CFT requirements.
 - Involvement in suspicious or illegal activities.
 - Significant changes in risk profile making the relationship untenable.
- Approval:
 - Obtain senior management approval before terminating any customer relationship.
 - Ensure that the decision is documented, including the reasons for termination.
- Documentation:
 - Maintain detailed records of the exit process, including:
 - Customer communication.
 - Internal approvals.
 - Steps taken to secure and retain records of the customer's transactions.
- Notification:
 - Inform the customer of the termination decision, ensuring compliance with contractual and legal obligations.
 - Provide a clear explanation unless prohibited by law (e.g., tipping-off regulations).
- Reporting:
 - Report the termination of high-risk customers to the relevant authorities, if required by law.
 - Document all reporting activities for compliance and audit purposes.

CASH ACCEPTANCE PROCEDURES

- For **AL NASER INTERNATIONAL** to mitigate the risk associated with cash transactions and ensure compliance with relevant AML/CFT regulations in the UAE. The following procedures will be followed:
- Threshold Limits:
 - Cash transactions exceeding AED 55,000 must be subjected to enhanced due diligence (EDD).
 - Any transaction close to the threshold should be scrutinized to avoid structuring (breaking transactions into smaller amounts to avoid reporting).

- Identification:
 - Obtain and verify a government-issued photo ID for all cash transactions.
 - Record the ID type, number, issuing country, and expiry date.
 - For transactions exceeding the threshold, collect additional documents to verify the source of funds such as bank statements / financial statements.
- Record Keeping:
 - Maintain records of all cash transactions including:
 - Customer identification details.
 - Amount, date, and purpose of the transaction.
 - Copies of identification documents and any additional verification documents.
 - Ensure records are kept for a minimum of five years after the transaction, as per Article 7 of the UAE Cabinet Decision No. (10) of 2019.
- Reporting:
 - Report any suspicious cash transactions immediately to the UAE Financial Intelligence Unit (FIU) using the goAML portal.
 - Ensure that all employees are aware of the reporting protocol and their responsibilities under Article 15 of the UAE Federal Decree-Law No. (20) of 2018.
- Training:
 - Regularly train employees on how to identify suspicious cash transactions and the procedures for reporting them.
 - Ensure the training includes real-life scenarios and case studies.

MAINTENANCE OF RECORDS & THEIR RETENTION

- **AL NASER INTERNATIONAL** will maintain all records, documents, data and statistics for all financial transactions and local or international commercial and cash transactions for a period of no less than five years from the date of completion of the transaction or termination of the business relationship with the Customer as required by the AML Law.
- The Company will keep all records and documents obtained through CDD measures, ongoing monitoring, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed , for a period of no less than five years from the date of termination of the business relationship or after the completion of a casual transaction or from the date of completion of the inspection by the Supervisory authorities, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.
- The records, documents and data kept shall be organized so as to permit data analysis and tracking of financial transactions.
- The Company will make all Customer information regarding CDD towards Customers, ongoing monitoring and results of their analysis, records, files, documents, correspondence and forms available immediately to the relevant authorities upon request.
- **AL NASER INTERNATIONAL** maintains 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.
- All CDD information and transaction records should be available swiftly to Competent Authorities upon appropriate authority.

Retention Period

AL NASER INTERNATIONAL's retention period for all records is at least five years, depending on the circumstances, 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 with **AL NASER INTERNATIONAL**;
- Completion of an occasional 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 form of termination of a legal person or arrangement.

Required Record Types

AL NASER INTERNATIONAL retains records which can be classified broadly into the following categories:

1. Transaction Records — This category relates to operational and statistical records, documents and information concerning all (commercial or financial) transactions executed or processed by the Company, whether domestic or international in nature.

2. CDD Records - This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:

- Customer Information, including account files and business correspondence, and results of any analysis undertaken;
- Company Information;
- Reliance on Third Parties to Undertake CDD
- Ongoing Monitoring of Business Relationships
- Suspicious Transaction Reports (STRs)

MONITORING SUSPICIOUS ACTIVITY

The Company has put in place indicators that can be used to identify the suspicion on the occurrence of the Crime in order to report STRs, and will update these indicators on an ongoing basis, as required, in accordance with the development and diversity of the methods used for committing such crimes, whilst complying with what the Supervisory Authorities or FIU may issue instructions in this regard.

In reporting the suspicious transactions, **AL NASER INTERNATIONAL** confirms to maintain confidentiality regarding both the information being reported and to the act of reporting itself and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

ONGOING MONITORING

To continuously monitor **AL NASER INTERNATIONAL's** customer transactions and activities to detect and prevent money laundering and terrorist financing in compliance with UAE law the following measures will be follow:

➤ Transaction Monitoring:

- Implement a robust transaction monitoring system capable of:
 - Real-time monitoring for high-risk transactions.
 - Periodic review of lower-risk transactions.
- Customize monitoring rules based on customer risk profiles and industry standards.

➤ Risk Reviews:

- Regularly review and update customer risk profiles.
- Perform enhanced reviews for high-risk customers at least annually or more frequently if needed.

➤ Alerts:

- Use systems to generate alerts for:
 - Large or unusual transactions.
 - Transactions involving high-risk jurisdictions.
 - Patterns indicative of money laundering or terrorist financing.
- Ensure alerts are reviewed and investigated promptly.

➤ Investigation:

- Investigate all alerts and suspicious activities thoroughly.
- Document the investigation process, findings, and actions taken.
- Escalate significant findings to senior management and report to the UAE FIU if necessary.

➤ Reporting:

- Report any confirmed suspicious activities to the UAE FIU using the goAML system.
- Ensure reports are comprehensive and include all relevant details.

➤ Training:

- Provide ongoing training to staff on the importance of ongoing monitoring.
- Include training on the use of monitoring tools and how to recognize suspicious activity.
- Update training programs regularly to reflect changes in regulations and emerging risks.

REPORTING TO FINANCIAL INTELLIGENCE UNIT

If the Company have reasonable grounds to suspect that a **Transaction, Attempted transaction, or Funds** constitute crime proceeds in whole or in part, or are related to the Crime or intended to be used in such activity, regardless of the amount, they shall adhere to the following without invoking secrecy:

- o Directly report STRs to the FIU without any delay, via the electronic system of the FIU or by any other means approved by the FIU.
- o Respond to all additional information requested by the FIU.

The Company assures that their managers, officials or staff, will not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor will they disclose the information or data contained therein, or that an investigation is being conducted in that regard.

Web Reporting Requirements: Dealers in Precious Metals & Stones Report (DPMSR)

- All **Cash transactions** with individuals equal or exceeding AED 55000.00 need to be reported in the GoAML System.
- Exceptions: (Not to Report) – Any Credit Card /Cheque or Bank Transfer transactions of any amount. Only if Suspicious then to be reported through STR Option in GoAML System.
- All Cash/ International Wire Transfers / Transfers through Exchange Houses or Remittance Companies equal or exceeding AED 55000.00 need to be reported in the GoAML System.
- All Settlements in USD with following qualifications.
- Both Entities having accounts in UAE and transfers done for USD payments.
- USD Settlements done between two Free zones Within UAE, having different bank accounts, and Settlements between Free zone and onshore companies registered in the UAE.

Exceptions: (Not to Report)

- AED Settlement where both the parties have accounts in same bank in the UAE.
- AED Settlement where both the parties have accounts in different banks in the UAE.
- USD Settlement where both the parties have accounts in same bank in the UAE.
- Trade between related parties Mainland to Free zone having same bank account transactions and Vice Versa.
- Barter transaction (Exchange of Gold)
- Intra Company Transactions

- Transaction not routed through the UAE Bank Account.

REPORTING PROCEDURES TO SENIOR MANAGEMENT

To ensure that **AL NASER INTERNATIONAL's** senior management is informed about significant AML/CFT issues and can take appropriate action as per UAE regulations the following measures will be conducted:

➤ Regular Reports:

- Submit detailed semi-annual reports to senior management covering:
 - Number and nature of suspicious transaction reports (STRs) filed.
 - Results of ongoing monitoring activities.
 - Updates on high-risk customers and EDD findings.
 - Compliance audit results.
- Include an assessment of the effectiveness of current AML/CFT measures.

➤ Incident Reporting:

- Immediately escalate any significant AML/CFT incidents (e.g., major breaches, high-risk findings) to senior management.
- Provide a detailed report outlining the nature of the incident, its impact, and proposed remedial actions.

➤ Review Meetings:

- Hold quarterly meetings with senior management to review AML/CFT compliance status and discuss emerging risks or trends.
- Ensure minutes are recorded and actions are tracked.

➤ Decision Making:

- Senior management should be involved in decisions related to:
 - Policy changes.
 - High-risk customer acceptance or termination.
 - Resource allocation for AML/CFT activities.

➤ Documentation:

- Maintain comprehensive records of all reports and communications with senior management regarding AML/CFT matters for at least five years.

INTERNAL AUDIT

Internal Audit shall ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of

exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front-line staff of their responsibilities in this regard.

- A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. **AL NASER INTERNATIONAL** confirms to have in place an independent audit function to test the effectiveness and adequacy of their internal policies controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organizations. The scope of such audits should include but not be limited to:
- Examine the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements,
- Assess training adequacy, including its comprehensiveness, accuracy of materials training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity.

INDEPENDENT / EXTERNAL AUDIT

To provide an independent assessment of the effectiveness of the AML/CFT program in compliance with UAE laws, **AL NASER INTERNATIONAL** will conduct the following procedures:

- Regular Audits:
 - Schedule independent audits annually.
 - Audits should cover all AML/CFT procedures, including CDD, EDD, transaction monitoring, and reporting.
- Scope:
 - The audit should evaluate:
 - Compliance with UAE laws and regulations.
 - Effectiveness of policies and procedures.
 - Accuracy and completeness of record-keeping.
 - Adequacy of staff training.
- Findings and Recommendations:
 - Document audit findings in a detailed report.
 - Provide clear recommendations for addressing any deficiencies or areas for improvement.

➤ **Action Plan:**

- Develop a corrective action plan based on the audit recommendations.
- Assign responsibilities and timelines for implementing corrective measures.

➤ **Follow-Up:**

- Conduct follow-up audits to ensure corrective actions have been implemented and are effective.
- Report follow-up findings to senior management.

EMPLOYEE'S TRAINING

AL NASER INTERNATIONAL has an ongoing employee training under the leadership of the Compliance Officer.

The training includes, inter alia:

- How to identify red flags and signs of money laundering that arise during the course of the employees' duties.
- What to do once the risk is identified?
- What are the employees' roles in the company's compliance efforts and how to perform them.
- The company's record retention policy; and
- The disciplinary consequences for non-compliance with the Act.

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

CONFIDENTIAL REPORTING OF AML NON-COMPLIANCE

The Managers, officials or staff, will not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard.

REVIEW

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

A regular review of the "Compliance Manual" shall be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources, and should be

accompanied by a formal assessment or written report. If and when regulations are amended concerning reporting of suspicious activities, **AL NASER INTERNATIONAL** will amend the Compliance Manual to comply with those regulations.

Scope:

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

COMMUNICATION

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

FINES & PENALTIES

As per Federal Decree – Law (20) of 2018

The Regulator has the authority to impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning

b) Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (five million dirham) for each violation.

- c) Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
- d) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
- e) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
- f) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.
- g) Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.

DISCLAIMER

Any employee who has reasons to believe that **AL NASER INTERNATIONAL** might be or has been exposed to funds from a doubtful source should come forward to management immediately.

Any employee who is found in violation of the terms of this Policy will be subject to disciplinary action.

Any employee with direct knowledge of potential or apparent violations of this Policy who fails to report such acts to Company management will also be subject to disciplinary action.

Any employee who knowingly misleads or hinders an investigation to reported violations of the Policy and any relevant and applicable law also may be subject to disciplinary action.

Disciplinary actions may risk termination of employment. The same applies to third-parties that are associated with **AL NASER INTERNATIONAL** operations. Third-parties risk having their contracts re-evaluated or terminated.

DATE OF REVISION AND UPDATE: 2 JANUARY 2024

ANNEXURE

#Glossary

CBUAE : Central Bank of the UAE

Committee : National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations.

FIU: Financial Intelligence Unit

Supervisory Authority: Federal and local authorities which are entrusted by legislation to supervise financial institutions, designated non-financial businesses and professions 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 legislations.

Law-enforcement Authorities : Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidence on the crimes including AML/CFT crimes and financing illegal organizations.

Crime: Money laundering crime and related predicate offences, or financing of terrorism or illegal organizations.

Funds : Assets in whatever form, tangible or intangible, movable or immovable including national currency, foreign currencies, documents, or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.

Proceeds : Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.

Means : Any means used or intended to be used to commit an offence or felony.

Suspicious Transactions: Transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanor or felony or related to the financing of terrorism or of illegal organizations, whether committed or attempted.

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.

Confiscation : Permanent expropriation of private funds or proceeds or instrumentalities by an injunction issued by a competent court.

Financial institutions: Anyone who conducts one or several of the activities or operations defined in the Implementing Regulation of the present Decree Law for the account of /or on behalf of a client.

Designated Nonfinancial Businesses and Professions: Anyone who conducts one or several of the commercial or professional activities defined in the Implementing Regulation of this Decree Law.

Legal Arrangement: A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as trust funds or other similar arrangements.

Client : Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law with one of the financial institutions or designated nonfinancial businesses and professions.

Beneficial Owner: The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or legal arrangement

Transaction: All disposal or use of Funds or proceeds including for example: deposits, withdrawals, conversion, sales, purchases, lending, swap, mortgage, and donation.

Registrar: The entity in charge of supervising the register of commercial names for all types of establishments registered in the UAE.

Customer Due Diligence (CDD): The process of identifying or verifying the information of a client or Beneficial owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it for the purpose of this Decree-Law and its Implementing Regulation.

Controlled Delivery : The process by which a competent authority allows the entering or transferring of illegal or suspicious funds or crime revenues to and from the UAE for the purpose of investigating a crime or identifying the identity of its perpetrators.

Undercover Operation : The process of search and investigation conducted by one of the judicial impoundment officer by impersonating or playing a disguised or false role to obtain evidence or information related to the Crime.

Wire Transfer : Financial transaction conducted by a financial institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.

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.

High Risk Customer : A Customer who represents a risk either in person, activity, business relationship, nature of geographical area, such as a Customer from a high-risk country or non-resident in a country in which he does not hold an identity card, or a customer 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.

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 include:
 - (a) Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP.
 - (b) Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.

Targeted Financial Sanctions (TFS): The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings, The term Targeted Financial Sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

The Executive Office: The Executive Office of the Committee for Goods and Materials Subject to Import and Export Control.

Local Terrorist List: Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) paragraph (I) of Federal Law No. (7) of 2014 on Combating Terrorism Offences.

UN Consolidated List: A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.

Without Delay: Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.