



AML/CFT Procedures and Controls



Clique Gold LLC



REVISION HISTORY

Document Name: AML/CFT Procedures and Controls
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	
Revision History.....	1
1.0 Introduction.....	4
2.0 The identification and assessment of ML/FT & PF risks	5
2.01 Risk Factors	5
2.02 Risk Assessment Methodology	5
2.03 Risk Assessment Operations	7
3.0 Customer Due Diligence.....	8
3.01 Customer On-boarding process and Customer Due Diligence measures	8
3.01.01 Identity Verification & Establishing CDD Profile	9
3.01.02 Risk Profiling.....	11
3.01.03 High-Risk Customers and Enhanced Due Diligence ('EDD') Measures ...	12
3.01.04 Ongoing Monitoring of Business Relationship	15
3.01.05 Exception to Customer Due Diligence	17
3.02 Reliance on Third Parties for CDD	17
3.03 Customer Acceptance Policy.....	18
3.04 Customer Exit Policy	18
4.0 Reporting of Suspicious Transactions/Activities.....	20
4.01 ML/FT and PF Red Flag indicators.....	20
4.02 Procedure and Timing for reporting suspicious transactions/activities and other information.	20
4.03 Handling business relationships after filing STR/SAR	22
5.0 AML/CFT Governance.....	25
5.01 Three lines of defense	25

5.02 AML/CFT Compliance Officer	25
5.03 Staff Screening and Training	27
5.03.01 Staff Screening and Employee Due Diligence	27
5.03.02 Staff Training	27
5.04 Independent Audit Function	28
5.05 Responsibilities of Senior Management	28
5.06 Maintenance of AML/CFT Registers.....	28
6.0 Record-keeping.....	29
6.01 Required Record Types.....	29
6.01.01 Financial Transactions	29
6.01.02 Customer Information.....	30
6.01.03 Reliance on Third Parties to Undertake CDD	30
6.01.04 Ongoing Monitoring of Business Relationships	30
6.01.05 Suspicious Transaction/Activity Reports (STR/SAR)	31
6.01.06 AML/CFT Training	31
7.0 International Financial Sanctions	32
7.01 TFS Implementation Steps.....	32

1.0 INTRODUCTION

In continuation to **Clique Gold LLC** AML/CFT Policy to fight money laundering and the financing of terrorism, the Company has designed adequate procedures and controls aimed at effective implementation of the AML/CFT Policies.

This document on AML/CFT procedures and controls must be read with the latest AML/CFT Policy of the Company. Compliance with the procedures and controls captured in this document is mandatory for all the executives and employees of the Company. Non-compliance with the procedural guidelines or mitigation measures mentioned in this document will lead to the corresponding responsibilities and sanctions.

In this document, the reference to AML/CFT shall by default include reference to CPF (Countering Proliferation Financing) unless specifically excluded.

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

The Company assesses its ML/FT and Proliferation Financing (PF) risks and adopting the risk-based approach, the necessary procedures and controls are defined and implemented across the Company.

2.01 Risk Factors

To precisely assess the risks and deploy the adequate measures, the Company considers the following parameters while assessing the ML/FT/PF risks, in line with the factors suggested in the National Risk Assessment (NRA), by the Supervisory Authorities, etc.:

- a. Client 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

Refer Annexure A to AML Procedures – Enterprise-Wide Risk Assessment Methodology and Enterprise-Wide Risk Assessment Chart

The Company shall annually conduct the AML Enterprise-Wide Risk Assessment (EWRA) or upon significant changes in the risk parameters, whichever is earlier.

2.02 Risk Assessment Methodology

The Company's risk assessment is done based on the combination of the following methodology:

- Risk assessment is in line with the management-approved risk appetite and policies.
- Risk assessment is based on the inputs from internal sources, including the designated AML/CFT Compliance Officer.
- Risk assessment considering relevant information (such as ML/FT & PF trends and sectoral risks) from external sources, including the NRA, Supervisory and other Competent Authorities, and international organizations such as FATF, MENAFATF, and other FSRBs, the Egmont Group, and others where appropriate.

While doing the risk assessment analysis, the following elements are given due consideration:

- Likelihood or probability of occurrence of identified risks,
- Timing of identified risks,
- Impact on the organization of identified risks.

Based on the ML/FT & PF Risk Assessment, identified risks are classified into high, medium, and low categories. This classification helps prioritize ML/FT & PF risk exposure and the appropriate types and levels of AML/CFT resources needed and adopt and apply reasonable and risk-proportionate mitigation measures.

Considering the size and nature of our business, we have identified the following processes for risk assessment:

- Obtaining and evaluating input from relevant internal sources, including AML/CFT Compliance Officer, such as internal meetings or interviews; review of internal audit reports.
- Obtaining and evaluating ML/FT & PF trends and sectoral risks from external sources, such as NRA, Supervisory Authorities, FIU, other national Competent Authorities, including international organizations, such as FATF, MENAFATF, and other FSRBs, the Egmont Group, and others.
- Evaluation of identified ML/FT & PF risks against the Company's management-approved risk appetite statement and policies.
- Understanding the risk-rating methodologies of purchased IT systems for the weighting of risk factors, the classification of risks into different categories, and the prioritization of risks.
- Evaluating the likelihood of occurrence of identified ML/FT & PF risks and determining its timing and impact on the Company.
- Time to time testing and auditing the effectiveness and consistency of risk methodologies and their outputs about statutory obligations by the AML/CFT Compliance Officer or independent third-party expert.

The processes mentioned above are subject to addition/modification as and when any new process for risk assessment is identified.

2.03 Risk Assessment Operations

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

The following information concerning the risk assessment is maintained:

- ML/FT risk assessment policies and procedures, including organizational roles and responsibilities; process flows, timing, and frequency; internal reporting requirements; and review, testing, and audit requirements.
- Risk assessment model or methodology used, and records related to its evaluation, testing, and updating, as relevant.
- Risk factors identified and input received from relevant internal sources, including the designated Compliance Officer.
- Details of the risk-factor analysis that constitutes the risk assessment.

Risk Assessment operations are updated on an ongoing basis and analysed based on risk identification and assessment analysis with supporting data.

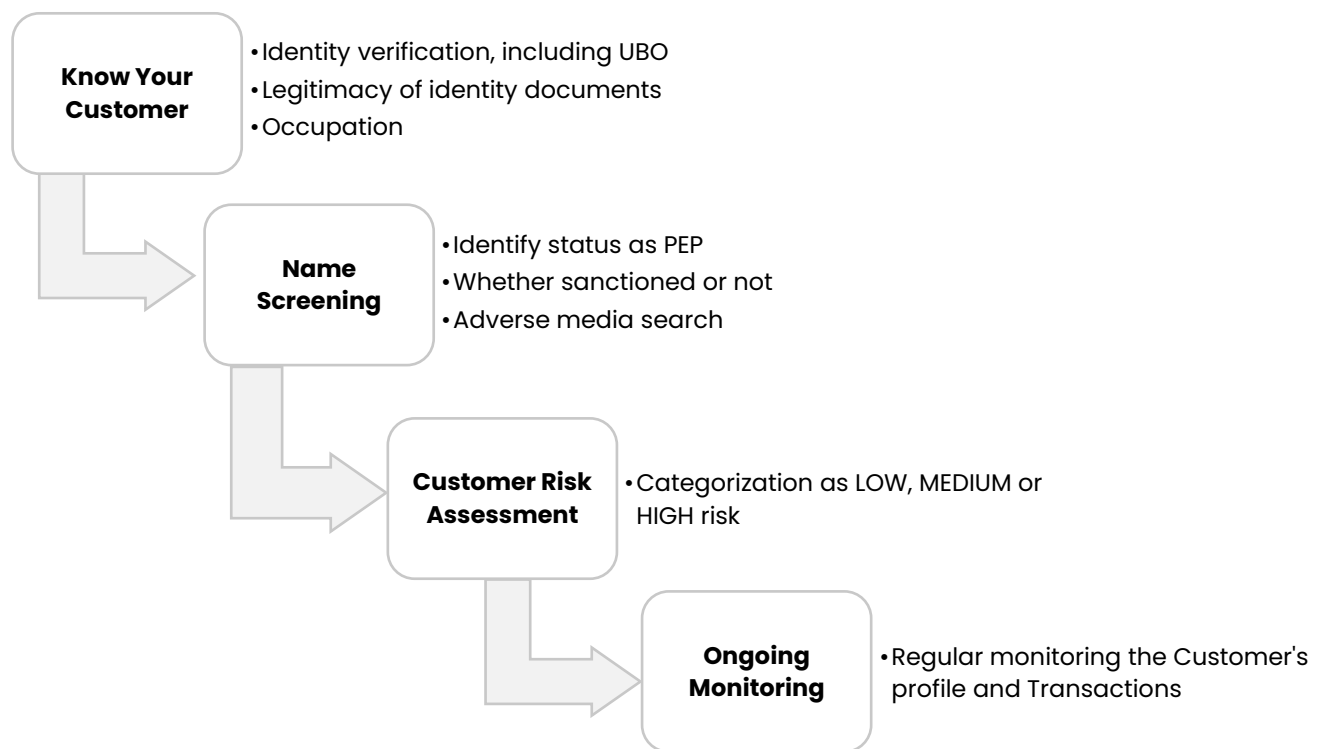
3.0 CUSTOMER DUE DILIGENCE

As part of the Company’s AML/CFT policy around Customer Due Diligence, the Company has designed the following procedures and controls to mitigate the ML/FT/PF risks:

Here, the “customer” shall include a reference to the customers, suppliers, beneficiaries, beneficial owners and controlling parties.

3.01 Customer On-boarding process and Customer Due Diligence measures

Customer Due Diligence process:



The Company has identified the activities which shall be performed as part of the CDD measure, depending upon the customer’s ML/FT risk classification.

Further, the CDD information shall be reviewed and updated based on the risk classification of the customer, as under:

- a. Customers with '**Low-risk**' category – In every 3 years, unless any information is gathered which indicates a change in the risk categorization,
- b. Customers with '**High-risk**' category – In every 12 months, till the risk category changes,

- c. Customers other than the above risk categories' **Medium-risk**' profile – In every 2 years, unless any information is gathered, which indicates a change in the risk categorization.

The Company's CDD measures shall comprise of following activities:

3.01.01 Identity Verification & Establishing CDD Profile

The Company shall follow the following measures for the identification of customers, suppliers, beneficial owners, beneficiaries, or controlling persons and verification of the identity based on documents and independent sources:

- a. Filling in the "Know Your Customer/Business" form as designed to capture the necessary details of the customers, suppliers, beneficial owners, beneficiaries, or controlling persons.
*Refer to **Annexure B** for Know Your Customer form.*
- b. The employee performing the verification shall also collect documents evidencing the following:
 - i. Identity of the person (such as government-issued document or passport),
 - ii. Nationality and national identification number,
 - iii. Trade License, in case of an entity or Company,
 - iv. Date & place of birth or establishment (as the case may be),
 - v. Address of residence or establishment, as may be applicable,
 - vi. Local residence address.
- c. Identity verification (government-issued document or passport) shall be done for signatories or representatives/attorneys in case of legal person or arrangement and parent/legal guardian in case of the customer being a minor.
- d. To verify the identity, the original identity document shall be sought for review, and a copy of the same shall be retained for recording purposes. In exceptional cases where the original document cannot be furnished, a copy certified as "true copy" of the original shall be sought.
- e. Further, in case of a customer is a legal person, the following additional details would be sought:

- i. Certificate of incorporation or registration,
 - ii. The articles of association, memorandum of understanding, or other equivalent governing documents, and
 - iii. Details of the senior management and board of directors.
- f. In case of the customer is a legal person owned or controlled by any other person, the Company has the policy to identify the Ultimate Beneficial Owners (UBOs) till the natural person holding **25%** or more of the ownership or controlling interest is identified.

In the UBO cannot be identified basis the ownership or the controlling interest, the Company shall consider the senior management of the customer as the UBO.

- g. Seeking documents and performing an independent search on public sites or through external sources to identify whether the customer is a Politically Exposed Person ('PEP'), or person associated with such PEP.
- h. Additionally, other details to be sought from the client shall include the type of activity they are engaged in.
- i. The Company shall also undertake screening to identify any potentially adverse information, such as criminal history.
- j. If a customer is a foundation, the following information would be sought and verified:
- Certified copy of the foundation's by-laws and charter,
 - Document evidencing appointment of the guardian,
 - Identity of the founder, contributors, guardian, beneficiary, any persons entitled to receive any assets or income from the foundation, and other natural person effectively controlling the foundation.
- k. In case of trust or customer having similar legal structure, the below-mentioned information would be obtained and verified:
- Certified copy of the Trust Deed, evidencing nature, purpose, and terms of the legal arrangement,
 - Document evidencing the appointment of the Trustee and the details about beneficiaries,

- Identity of the settlor, trustee, protector, enforcer, beneficiaries, and other natural person effectively controlling the trust fund.

The Company shall document the KYC form filled for a customer, along with the documents obtained from the customer or independent sources. Also, such procedure shall include certification by the employee performing the verification, their designation, time and date of verification, and the person who reviewed the customer identification documents.

The Company strictly adheres to the requirement of identification of beneficial owner. The Company shall not onboard or transact with a legal person where one or more of the beneficial owners of the customer are not known.

3.01.02 Risk Profiling

The Company shall classify the customer’s risk basis the following factors, including considering the outcome of the customer screening results:

- Nature of the customer
- The geographies the customer is associated with.
- The nature of the transaction, including the services to be provided.
- Delivery channels involved, including the way the customer is onboard.
- Other relevant risk factors

the risk classification of each risk scenario and the risk factor shall be done considering the weightage risk significance of each risk factor, as determined while conducting the Enterprise-Wide Risk Assessment. Here, the risk classification shall be done as under:

Risk Classification	Condition
Low	When Customer’s Factor-specific Risk Score is less than the EWRA’s Average Risk Score
Medium	When Customer’s Factor-specific Risk Score is between Average Risk Score & EWRA’s Factor-specific Risk Score
High	When Customer’s Factor-specific Risk Score is greater than EWRA’s Factor-specific Risk Score

While the overall customer’s risk profiling is done considering the following:

- Risk Factor-specific score
- Customer’s Weighted Average Risk Score to the Total Risk Score
- EWRA’s Average Risk Score
- Any exceptional condition warranting to specifically classify the customer as “High” or “Unacceptable”

The criteria for risk scoring and the classification of the customer’s risk category the same are mentioned in the “Risk Profiling” form.

Refer **Annexure B** – Risk Profiling Corporate and Individuals.

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

As part of the Enhanced Due Diligence measures, the Company shall apply the following process:

EDD FOR HIGH-RISK CUSTOMER

EDD involves the more rigorous application of CDD measures with respect to high-risk customers and transactions, which includes:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources about customer identity,
- 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 source of wealth, and the purpose of individual transactions,
- Requiring 1st payment to be carried out through an account in customer's name with a bank subject to similar CDD standards,
- Increased supervision of the Business Relationship, including the requirement for higher levels of management approval, more frequent monitoring of transactions as mentioned above, and more frequent review and updating of CDD information,
- The Company performs thorough background search using the following:
 - o Manual internet search protocols,
 - o Public or private databases,
 - o Publicly accessible or subscription information aggregation services.

Any business relationship with identified high-risk customers shall be established only after obtaining approval from the senior management of the Company.

HIGH-RISK COUNTRIES

For the purpose of high-risk countries, the Company refers to the countries defined so by UAE's National Anti-Money Laundering and Combating of Financing of Terrorism and Illegal Organizations Committee (NAMLCFTC). This includes the list of countries subject to United Nations' Targeted Financial Sanctions as prescribed at **Annexure C** and the jurisdictions captured under FATF's Blacklist and Grey list as prescribed at **Annexure D**. For these countries, the risk score assigned will be higher than the risk score for the other countries and the decision whether to apply EDD measures or not shall be determined basis the overall risk classification of the customer.

The Company shall adequately file any of the following reports, when remittances are originating from or destined to or routed through the high-risk countries subject to FATF Call for Action (also known as countries on FATF "Blacklist") (Refer **Annexure D**):

- a. **High-Risk Country Transaction Report (HRC):** If a customer hails from high-risk country, then the transaction with a such customer, whether at the time of establishing a relationship or during the customer relationship, then the Company shall submit an HRC with the FIU. In such a case, the Company shall ensure that the reported transaction shall only be executed if the FIU does not object to the transaction, and that too after three working days after filing an HRC.
- b. **High-Risk Country Activity Report (HRCA):** At the time of the establishment of a business relationship or during the customer relationship, if the Company observes any activities related to high-risk countries, then the Company shall submit an HRCA with the FIU. Here, such reported activities shall only be carried out after three working days from the date of reporting, only if the FIU does not object to the same.

EDD FOR POLITICALLY EXPOSED PERSONS ('PEP')

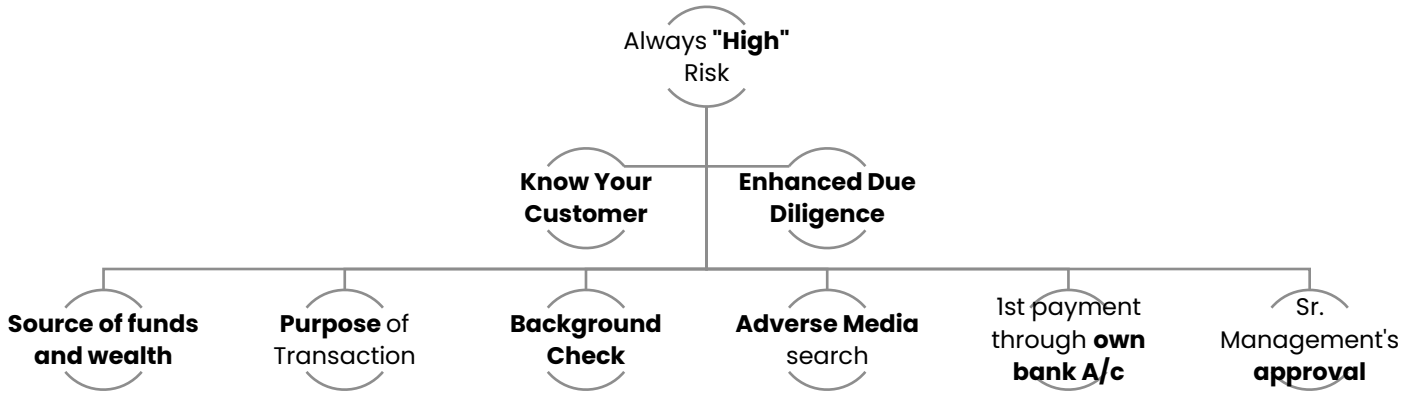
The Company shall classify the following persons as PEP:

- Person entrusted with prominent public functions in the UAE, or foreign country (Heads of government, senior politicians, senior government officials, judicial or military officials, senior executives of government-owned corporates, etc., and
- A person holds the senior management position in any international organizations or charged with administration of such international organizations like United Nations.

For customer identified as PEP, the below mentioned EDD measures shall be applied:

- For identifying whether a customer or the Beneficial Owner is a PEP, the KYC form designed by the Company has a specific field where the customer must give a declaration in that regard.
- The Company establishes the legitimacy of source of funds and source of wealth of PEP and also to investigate the individual's professional and financial background before becoming a PEP.
- Requiring 1st payment to be carried out through an account in customer's name with a bank subject to similar CDD standards,
- Prior to establishing a business relationship with PEP or executing any transaction with PEP, the Company has the policy to obtain approval from the senior management.

Summary of on-boarding PEP customer:



EDD FOR NON-PROFIT ORGANIZATIONS

As Non-Profit Organizations ('NPO') often pose increased risks regarding money laundering and financing of terrorism, the CDD procedure for the same includes the following measures:

- Ensuring that the NPO is properly licensed or registered,
- Assessing the adequacy of the NPO's AML/CFT policies, procedures, and controls,
- Obtaining information about NPO's:
 - Legal, regulatory, and supervisory status,
 - Requirements relating to regulatory disclosure, accounting, financial reporting, and audit,
 - Ownership and management structure,
 - Nature and scope of its activities,
 - Nature of its donor base as well as that of the beneficiaries of its activities and programs,
 - The geographic areas in which it operates.

As part of EDD, the employees of the Company shall perform thorough background checks (using internet searches, public databases, national/international sanctions, or subscription information aggregation services) of the NPO's senior management, major donors, and major beneficiaries.

Details pertaining to business relationships established with NPOs should be adequately documented, senior management approved, and communicated to the relevant employees of the Company.

3.01.04 Ongoing Monitoring of Business Relationship

As part of the ongoing monitoring and auditing of the transactions and customer's due diligence information, the Company shall obtain sufficient information to determine the transaction's reasonableness and legitimacy. Also, necessary information and documents are obtained by the Company for continuous screening of the customer's profile, along with the transactions.

For ongoing monitoring, the Company has set up the following rules:

a. **Threshold-based Rules:** Once the aggregate amount of the all the transactions with a single customer exceeds the **AED 300,000**, the said business relationship shall be monitored closely.

b. **Location-based Rules:**

Transactions with the UAE Non-Resident customers hailing from high-risk countries as defined under **Annexure C** and **Annexure D** shall be closely monitored once the aggregate value of the transaction per customer exceeds **AED 100,000**.

The said of countries under Targeted Financial Sanctions and Countries Subject to Call for Action/Jurisdictions under Increased Monitoring shall be updated by the AML/CFT Compliance Officer as amended by the relevant authorities and FATF.

c. **Transaction-based Rules:**

All the transactions wherein the value appears to be disproportionate to the size of the entity or financial profile of the customer shall be closely examined.

d. **Customer-based Rules:**

All transactions with high-risk customers are closely examined.

During ongoing monitoring, if any of the following circumstances are being observed, such transaction or business relationship shall trigger a special review and updating the CDD information:

- Discovery of information about a customer that is either contradictory or otherwise puts in doubt the appropriateness of the customer's existing risk classification or the accuracy of previously gathered data,
- Expiry of a customer's or Beneficial Owner's identification documents,
- Material changes in ownership, legal structure, or data such as name, registered address, purpose,

- Initiation of legal or judicial proceedings against a customer or Beneficial Owner,
- Finding materially adverse information about customers or Beneficial Owners, such as media reports about allegations or investigations of fraud, corruption, or other crimes,
- Qualified opinion from an independent auditor on the financial statements of a legal entity customer,
- Transactions that indicate potentially unusual or suspicious patterns of activity.

Update to Customer Information:

The update to the CDD information shall be done based on the verification of the source of fund and source of wealth of the customer, purpose of the transaction, nature of the customer's business, and review of the **last 2** transactions, executed with the customer.

e. Ongoing Sanctions screening:

As part of ongoing monitoring, the customers, UBOs, controlling parties and their businesses would also be regularly screened against the UN Sanctions List, the UAE Local List, and other relevant international sanctions.

- Regular and Ongoing Screening of the local as well as international Sanction List to identify if the person is listed therein.
- Screening should be conducted in the following circumstances:
 - Pursuant to any update in the Local terrorist list or UN consolidated List
 - Before onboarding of new customers
 - Prior to the processing of transactions
 - Changes in KYC information of the customer

f. Review of Ongoing Monitoring program and rules:

The Company shall review the defined rules, logic, and overall transaction monitoring program **annually**, to ensure its quality and effectiveness.

The Compliance Officer shall be responsible for conducting such a review and implementing necessary changes to enhance the quality of the transaction monitoring program.

3.01.05 Exception to Customer Due Diligence

The Company is also engaged in the trading of commodities (other than precious metals), services which are not prescribed under the AML/CFT Law and Decision as subject to any AML compliance by the Company as a DNFBP.

In such cases when the customer is expected to engage with the Company for products not regulated under AML, the Company shall restrict its Customer Due Diligence measures as described hereunder:

1. Obtaining a copy of the valid identity document of the client, their UBOs (including the person for whom the visa application is processed),
2. Screening the client against the Sanctions Lists,
3. Classifying the client as “Low risk” unless any risk indicator is observed suggesting otherwise,
4. Applying additional measures in case any matches with the Sanctions Lists are found or any other red flags related to ML/FT/PF is observed (i.e., classifying as high-risk and conducting complete CDD or if required, Enhanced Due Diligence).

3.02 Reliance on Third Parties for CDD

While relying on the CDD process performed by third parties, the Company shall ensure the adherence to the AML/CFT Decision and Law by the third parties by the following means:

- Comprehensiveness and quality of the policies, procedures, and controls implemented by the selected third party,
- Number of personnel dedicated to customer due diligence by such third party,
- Third party's audit and quality assurance policies with respect to CDD,
- Third party's regulatory and supervisory status as well as the good standing,
- Entering into a Service-level agreement to clearly set out the roles and responsibilities; nature of the CDD to be performed, and record-keeping requirements,
- The CDD performed by the third party shall be duly documented and shared with the company after certification by the senior management of the third party on real-time basis through an email or through electronic mode (such as cloud storage) after undertaking the CDD procedures. This shall include the true copies of the original documents collected by the third party from the customer during CDD.

The Company shall periodically review and document the above processes performed to ensure the adequacy of the record-keeping and adherence to the AML/CFT regulations by third parties.

In the circumstances where the Company is not satisfied with the identification and verification process carried out by the third-parties or the same is not aligned with the

AML/CFT Laws, then the Company itself shall conduct the entire CDD again or fill up the gaps in the process carried out by the third-party. The Company only shall be responsible for the customer due diligence measures.

3.03 Customer Acceptance Policy

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

- Accept only those customers whose identity is established by conducting due diligence appropriate to the risk profile of the customer.
- Where the customer is a new customer, it can only be onboarded after ensuring that pre-account opening KYC documentation, Screening, and Risk Assessment procedures are conducted.
 - (a) Documents as per standard norms to be collected.
 - (b) identity verification of the customer is performed.
- In the case of customers categorized as "high" risk, the business relationship shall be established only upon completion of the Enhanced Due Diligence measures.
- Signoff is obtained from the compliance team to onboard the customer.

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

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

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

3.04 Customer Exit Policy

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

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

- when the customer gets associated with “high-risk” countries as mentioned under the FATF Blacklist (*Refer **Annexure D***),
- when the ML/FT/PF risks associated with the customer exceeds the Company’s risk appetite.

When the Company concludes that it is not able to serve the customer anymore, it will treat the customer fairly and communicate in plain language.

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

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

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

4.0 REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

The Company has developed and deployed the following procedures and controls to ensure timely reporting of the identified suspicion:

4.01 ML/FT and PF Red Flag indicators

For identifying the suspicion of a crime involving ML/FT and PF, we have identified certain indicators as 'red flags' mentioned at **Annexure E** and **Annexure F** respectively, which need immediate attention of the Company's senior management and evaluation of the appropriateness of the risk classification of the customer.

The Company shall review and update the ML/FT and PF risk indicators **annually** from the date this policy comes into effect. Further, the modifications suggested by the Compliance Officer shall be reviewed and approved by the Senior Management of the Company. Also, if need be, the form designed for "Risk – Profiling" shall also be updated.

4.02 Procedure and Timing for reporting suspicious transactions/activities and other information.

The Company shall report the suspicious transactions through the electronic system of the FIU after choosing from the list the suspicious indicators at the time of filing the Suspicious Transaction Report ('STR') or Suspicious Activity Report ('SAR') without any delay. Such STR/SAR shall be filed with FIU by the CO appointed by the Company after due review, scrutiny, and study of the records and obtained data pertaining to Suspicious Transaction.

In case of suspicion, the concerned employee should report the same to the Compliance Officer in the form of an Internal STR or SAR, who shall review and determine the nature of the suspicion and whether the reporting is to be done with FIU.

The entire process should not take time of more than **48** working hours, from the point in time when there are reasonable grounds to suspect the transaction of the involvement of criminal activities related to money laundering and financing of terrorism. Once the decision has been made to report the suspicious transaction to FIU, there shall not be any delay in filing the report.

The Company shall ensure that the following details are submitted in the STR or SAR with utmost accuracy:

- Details of the transaction or activity which the Company considers as suspicious,
- Parties involved,
- Potential red flags and reason why the Compliance Officer considers the transaction or activity as suspicious,
- Action taken by the Company upon observation of the potential ML/FT/PF indicators.

While submitting the STR or SAR on the goAML Portal, the Compliance Officer shall attach the necessary documents relevant to the suspicion being reported.

The overall workflow for SAR/STR Submission Process is as follows:

Detection of Suspicious Activity/Transaction

- Company's personnel identifies a suspicious activity/transaction



Notification to the Compliance Officer

- The personnel notifies the Compliance Officer as to the suspicious activity/transaction in the SAR/STR Templates maintained for this purpose



Verification & Confirmation

- The Compliance Officer verifies the information and considers whether to file SAR/STR with the FIU



SAR/STR Submission

- The Compliance Officer files the SAR/STR with the FIU

However, in case there is a suspicion because the customer is not providing the required identification or address proof related information or source of funds and source of wealth after serving him the Request for Information (RFI), a reasonable period must be granted to the customer to provide the required information. The duration of reasonable time would depend on the facts of the case and the timing of serving the RFI.

The necessary actions should be taken in a way that confidentiality is maintained regarding the information being reported and the act of reporting the transaction to FIU itself.

Also, if any employee of the Company is found to have been involved in "tipping off", i.e., have informed the customer or any other person outside the Company about the reporting made to FIU or the information or data contained in the STR/SAR or fact that investigation is underway, strict actions shall be initiated against such an employee, which may include suspension of the employment contract with the Company for the certain time period and/or monetary fines up the AED 500,000.

4.03 Handling business relationships after filing STR/SAR

As soon as an STR/SAR has been filed by the AML/CFT Compliance Officer of the Company, the customer shall immediately be classified under the "High-Risk" category, and Enhanced Due Diligence shall be performed.

Further, the Company is obliged to follow the instructions given by FIU following the STR/SAR filed by the Company, such as:

- Instructions to reject the transaction,
- Instructions to allow the transaction to proceed (for ease in tracing the customer by the Competent Authorities),
- Instructions related to the seizure or freezing of Funds or other assets related to the customer,
- Instructions to terminate the business relationship,
- Instructions to maintain and monitor the business relationship and periodically or conditionally report activities related to it to the FIU and/or other Competent Authorities,
- Requests for additional information about the reported transaction, other transactions related to the customer, or about the business relationship in general.

As part of this policy, the designated AML/CFT Compliance Officer is obliged to maintain the confidentiality of the FIU's instructions, except for sharing the details of the FIU instructions with the Company's senior management.

Had there been any delay in receiving the instructions from FIU, the Company would make its best efforts to delay the execution or completion of the transaction reported in STR/SAR if such transaction is anticipated or pending or in progress. We have listed hereunder the suggested measures which the employees may resort to delay the execution or completion of the transaction:

- Delaying processing of the transaction without explanation for as long as possible.
- Advising the customer that the transaction has been delayed due to an unspecified operational, technical, staff, or other problem and that efforts are underway to resolve it.
- Requesting additional information and/or supporting documentation relating to the transaction, the customer, or the counterparty.
- Advising the customer that paperwork related to the transaction has been lost and requesting that it be resubmitted.
- Advising the customer that the transaction is pending an internal approval process.

- Any other reasonable delaying tactics, bearing in mind the obligation to avoid "tipping off" the customer.

If any additional suspicions are observed during the time wherein the transaction execution/completion is being delayed, then such additional suspicions should be reported to FIU as a follow-up to the original STR. Additional suspicion may arise due to any of the following reasons:

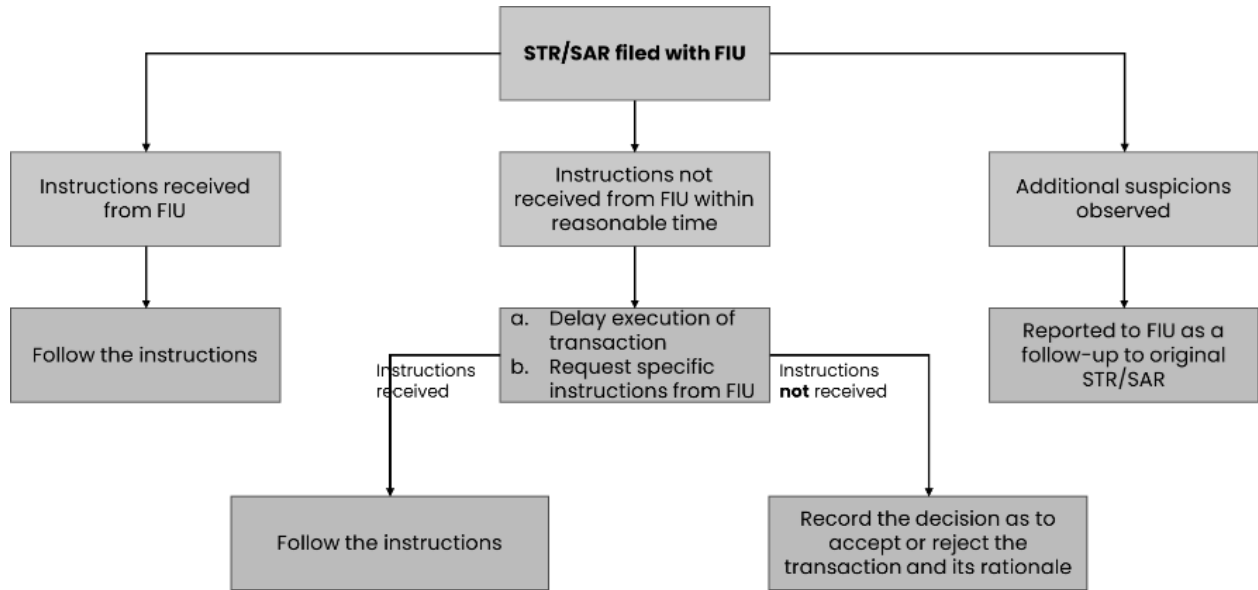
- New adverse information obtained in relation to the transaction, the business relationship, or the counterparty to the transaction.
- Sudden material amendments or changes to the circumstances or details of the transaction.
- Excessive pressure, intimidation, displays of anger or threats of any kind, forcing the Company to complete the transaction.
- Abrupt cancellation of the transaction, termination of the business relationship, or sudden attempts to withdraw or obtain a refund of the balance of deposits, funds, or other assets held by the Company.
- Any other reasonable grounds indicating that the customer has become aware that the transaction has been reported as suspicious.

If no instructions have been received from FIU even after a reasonable time, the Company, through Compliance Officer, shall request specific instructions or permission from the FIU regarding executing or rejecting the transaction.

Even after a specific request, if no instructions are received from the FIU and if we decide to maintain the relationship with the customer, we shall document the rationale for doing so and also implement necessary Enhanced Due Diligence measures to mitigate the associated ML/FT risks. Also, there shall be below mentioned restriction on the volume of transactions that can be permitted with such customers:

- a. Number of maximum transactions: **One (1)**,
- b. Cumulative value of transactions: Not exceeding **AED 10,000**.

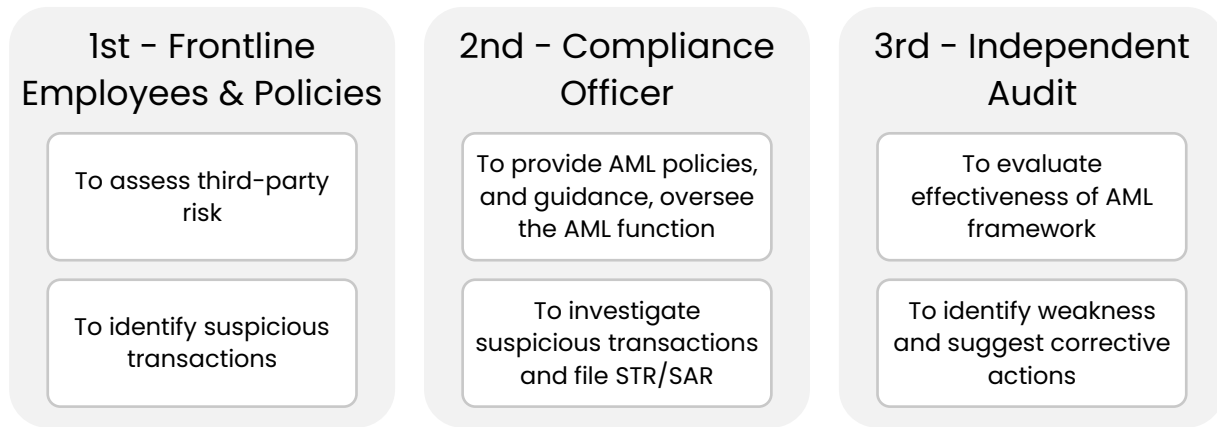
Overall guidelines on managing business relationship post filing of SAR/STR:



5.0 AML/CFT GOVERNANCE

5.01 Three lines of defense

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



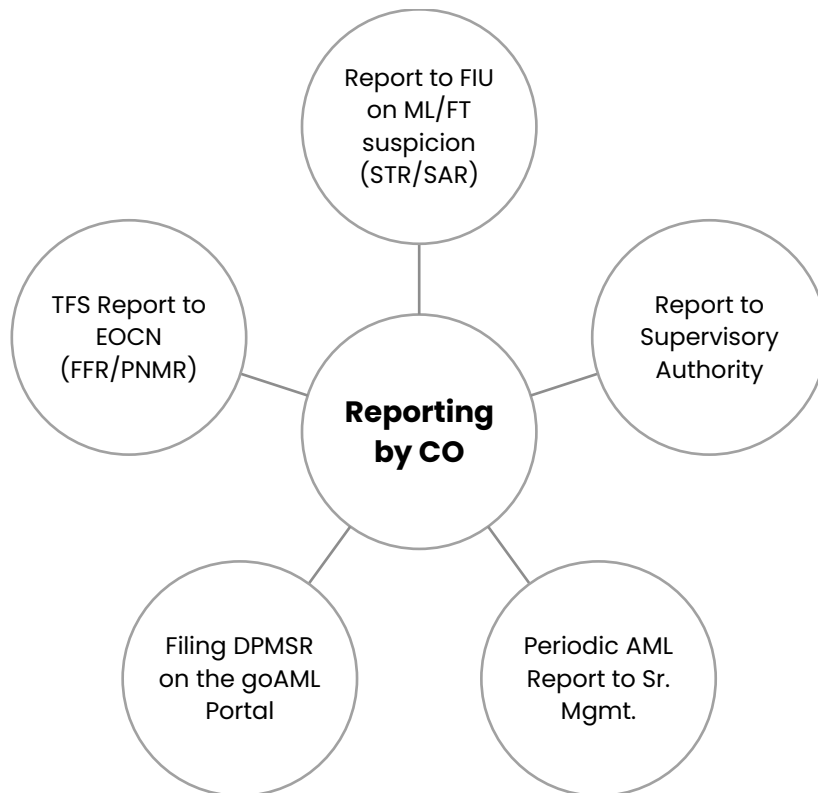
5.02 AML/CFT Compliance Officer

The AML/CFT Compliance Officer of the Company shall be responsible for undertaking the following functions, to ensure effective implementation of the AML/CFT Policy of the Company designed in accordance with the AML/CFT regulations:

- a. **AML/CFT Program Management:** To ensure the quality, strength, and effectiveness of the Company's AML/CFT program, the Compliance Officer ('CO') shall design and implement appropriate AML processes, procedures, and guidelines. Such an AML framework shall be reviewed and updated annually by the CO. CO shall be coordinating with the employees of the Company in relation to the identification of suspicious activity or transaction.
- b. **ML/FT Reporting:** The CO would be ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organizations for reporting suspicions to the FIU. Further, CO shall also cooperate with the Competent Authorities in relation to the performance of their duties regarding AML/CFT by providing the documents requested.

The Compliance Officer shall also furnish a semi-annual AML/CFT report to the senior management of the Company, capturing details pertaining to AML/CFT Compliance, any observed non-compliance, measures required for improving the compliance level in the organization. Such bi-annual reports on AML/CFT provisions shall be furnished with the Supervisory Authority, along with Senior Management’s comments and decision.

Further, the Company shall also furnish Dealers in Precious Metals and Stones Report (DPMSR) on the goAML Portal when the purchase or sell transaction is settled in cash or international wire transfer of AED 55,000 or more, within 2 weeks from the date of receipt or payment of such amount.



- c. **AML/CFT Training and Development:** As part of AML/CFT training program, the Compliance Officer would include senior management and other internal and external stakeholders to ensure that the Company’s employees are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

5.03 Staff Screening and Training

5.03.01 Staff Screening and Employee Due Diligence

As part of the "Employee Due Diligence", the Company shall adopt the following measures to ensure that competent team is managing the business operations, and specifically AML Compliance:

- The Company shall obtain the identity details of the employee, including supporting valid documents.
- Employee's identity shall be adequate verified by the Human Resource team of the Company.
- Necessary screening shall be performed of all the employees to check if the person is sanctioned or connected to the sanctioned person or associated with a PEP.
- Inquiry and investigation shall also be conducted to understand the background of the person – financially as well as criminal history.

The Company shall also seek references from previous employers of the person about the behaviour and attitude towards compliance.

5.03.02 Staff Training

All the employees of the Company dealing with customers, employees who could be able to encounter suspicious activities, and the senior management would be required to undertake mandatory training on AML/CFT regulations, their roles and responsibilities under the law, and necessary compliance obligations. Such training must be completed as part of job orientation.

The training modules shall be designed considering the outcome of the Enterprise-Wide Risk Assessment conducted by the Company, the types of services or products being offered, and the level of complexity of the transactions.

The training shall be delivered by the CO, or third-party trainers as may be appointed by the CO. The training module shall cover the following:

- The AML/CFT regulations covering aspects of money laundering and terrorist financing.
- Company's internal policy and procedures relating to AML/CFT.
- Guidance on identifying the transaction involving money laundering and terrorist financing.
- Internal reporting of any suspicious transactions to CO.
- Awareness about the roles and responsibilities of each employee towards fighting money laundering and combating terrorism financing.

5.04 Independent Audit Function

The Company shall appoint an independent AML auditor, who shall perform periodic inspection and testing of all aspects of our AML/CFT compliance programs, including ML/FT risk assessment and mitigation measures and customer due diligence policies, procedures, and controls.

The independent auditor's report on AML/CFT program of the Company shall be directly presented to the Senior Management.

5.05 Responsibilities of Senior Management

The Compliance Officer shall conduct periodic awareness sessions with the senior management of the Company around the senior management's roles and responsibilities towards AML/CFT compliance program.

5.06 Maintenance of AML/CFT Registers

The Compliance Officer shall ensure maintenance of the following registers from AML/CFT perspective:

- Customer Register
- Transaction Register, including reference to the transactional reports (DPMSR) furnished on the goAML Portal
- Employee Register
- Register pertaining to various goAML reports:
 - o Suspicious Transaction Report (STR)
 - o Suspicious Activity Report (SAR)
 - o Fund Freeze Report (FFR)
 - o Partial Name Match Report (PNMR)
 - o High-Risk Country Transaction Report (HRC)
 - o High-Risk Country Activity Report (HRCA)

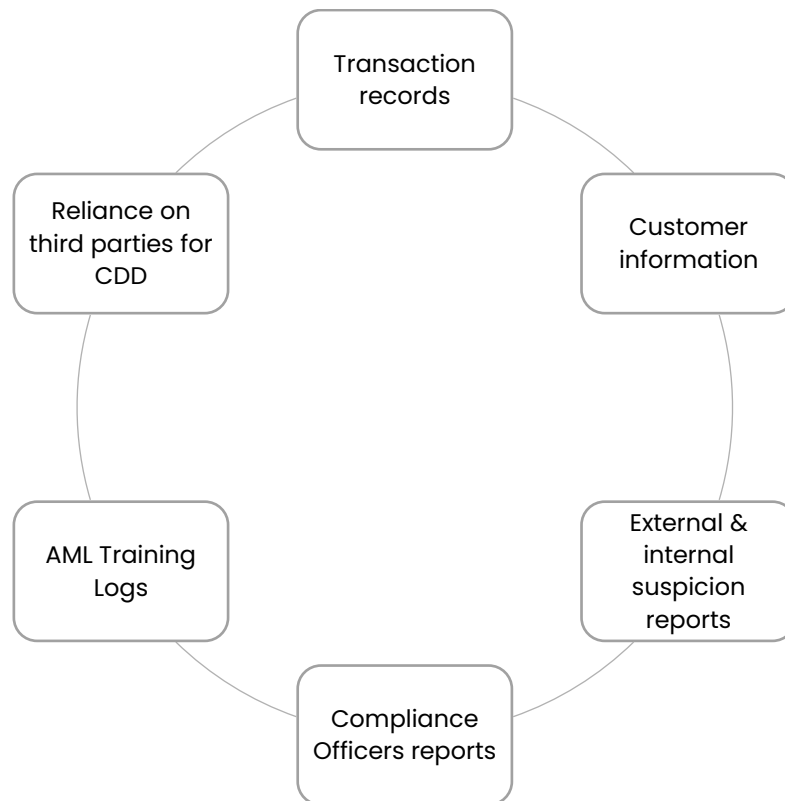
The overall AML compliance functions of the Company are listed as **Annexure G**.

6.0 RECORD-KEEPING

All the AML/CFT related records must be maintained in an organized manner in soft copies wherever possible. If not, the physical copy of the same should be maintained, duly signed by the employee-in-charge, and verified by the Compliance Officer. No data pertaining to AML/CFT shall be archived or transferred or destructed without the approval of the CO and the senior management.

6.01 Required Record Types

On the basis of the types of records to be maintained by the Company with respect to AML/CFT, the Company has designed the policy for each of the categories of the records:



6.01.01 Financial Transactions

We shall maintain the operational and statistical records concerning all financial transactions executed or processed by the Company for a minimum period as prescribed in the AML/CFT Policy, which shall include the following:

- Customer correspondence, requests, or order forms related to initiation and performance of all types of transactions,
- Customer payment advice, receipts, invoices, billing notifications, bills of exchange, statements of account, expense reimbursement requests or notifications,
- Escrow or fiduciary account transaction records,

- Supply of services, lease, and similar agreements,
- Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

6.01.02 Customer Information

The Company shall be retaining all customer records and documents obtained through the performance of CDD measures in relation to Business Relationships, including customers, Beneficial Owners, beneficiaries, or other controlling persons.

- Customer account information and files,
- Customer correspondence, call reports or meeting minutes,
- Copies of personal identification documents, KYC and CDD (including EDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries, and investigations,
- Customer risk assessment and classification records.

6.01.03 Reliance on Third Parties to Undertake CDD

If third parties are involved in undertaking CDD, the company shall ensure that copies of all necessary documents collected through the performance of CDD measures can be obtained upon request and without delay and that the third parties adhere to the record-keeping requirements of the AML-CFT decision.

The CO of the company shall:

- Assess, monitor, and test third party's policies, procedures, and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures,
- Specify service-level agreements with third parties governing the provision of record-keeping services,
- Determine Operational procedures related to request and transfer of records and documents, as well as their physical and cyber security, and the protection of active and archived data and records from unauthorized access,
- Prepare audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.

6.01.04 Ongoing Monitoring of Business Relationships

The Company shall be retaining all customer records and documents obtained in the course of ongoing monitoring of Business Relationships:

- Transaction review, analysis, and investigation files, with related correspondence,

- Customer correspondence, call reports, or meeting minutes (recordings, transcripts, or logs of calls) related to transactions or their analysis and investigation,
- Customer due diligence records, documents, profiles, or information gathered in the course of reviewing, analyzing, or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions,
- Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.

6.01.05 Suspicious Transaction/Activity Reports (STR/SAR)

We have the policy to retain all records and documents pertaining to suspicious transaction reports and the results of all analysis or investigations performed. This shall relate to both internal STRs or SARs and those filed with the FIU by the CO and include the following:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence,
- Competent authority request for information and their related investigation files and correspondence,
- CDD and Business Relationship monitoring records, documents and information obtained while analyzing or investigating potentially suspicious transactions and all internal or external correspondence or communication records associated with them,
- STRs (internal and external), logs, and statistics, together with their related analysis, recommendations, decision records, and all related correspondence,
- Notes concerning feedback provided by the FIU with respect to reported suspicious transactions, as well as notes or records pertaining to any other actions taken by, or required by, the FIU.

6.01.06 AML/CFT Training

The Company shall maintain the training log of all the trainings conducted for the employees related to AML/CFT. The details should be captured in the records would be as under:

- Date and duration of the training session,
- Topic covered during the training session,
- Mode of training and the details of trainer,
- Details of the staff who attended the training.

7.0 INTERNATIONAL FINANCIAL SANCTIONS

To comply with the provisions of Cabinet Decision No. (74) of 2020, and effectively implement the Targeted Financial Sanctions ('TFS'), the Compliance Officer shall:

- Identify, understand, assess, monitor, and manage the risks associated with TFS and other international financial sanctions regimes and restrictive measures.
- Establish information and operating systems, procedures, and controls pertaining to customer and Business Relationship screening, alert management, escalation, and reporting related to TFS and other international financial sanctions regimes and restrictive measures.
- Establish information and operating systems, policies, procedures, and controls related to the implementation of the requirements of TFS and other international financial sanctions regimes and restrictive measures.
- Adhere to staff training and awareness-building requirements pertaining to TFS and other international financial sanctions regimes and restrictive measures.
- Establish appropriate independent audit policies and testing procedures with respect to the operational and control framework for TFS and other international financial sanctions regimes and restrictive measures.

7.01 TFS Implementation Steps

The Company shall conduct the regular and ongoing Screening of the local as well as international Sanction List to identify if the customer, supplier, beneficial owners, controlling parties or any of the Company's employee is listed therein.

The AML/CFT Compliance Officer shall subscribe to the Executive Office for Control and Non-Proliferation (EOCN) Notification System to receive automated notifications around updates made to the Local Terrorist List and UN Consolidated List. The CO shall respond to such notifications received around additions/delisting of the designated persons, as required by the EOCN.

Further, the screening shall be conducted in the following circumstances:

- Pursuant to any update in the Local terrorist list or UN consolidated List
- Before onboarding of new customer
- Prior to the processing of transactions
- Changes in KYC information of the customer

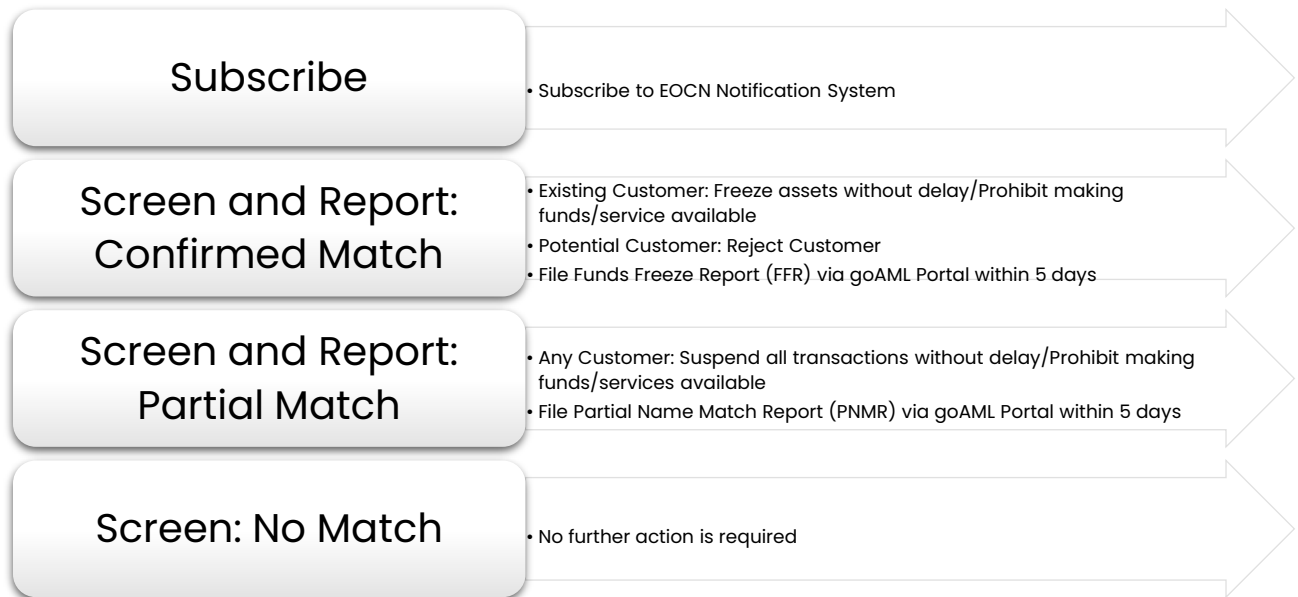
While submitting the report (FFR or PNMR) on the goAML Portal, the Company shall adequately capture the following details:

- Details about the parties involved.
- Whether the screening results suggest 'confirmed match' or 'potential match'.
- Whether the Company has applied any freezing measures. If yes, the amount of funds frozen.

Even in case the Company has no access to the designated person's fund and no freezing measures are applied, the FFR is to be filed and remark around non-freezing of funds shall be clearly captured.

- Transactional details, in case the designated person is the existing customer.

Following is the detailing of the steps how the Company shall implement the Targeted Financial Sanctions requirements:



AML/CFT Procedures and Controls approved by:

Signature:

Name:

Designation: