

Anti-Money Laundering Policy (AML)

This policy has been formed in the light of SEBI Circulars–on Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) as amended – obligations of Intermediaries under the **Prevention of Money Laundering Act, 2002 ('Act')** and **Rules** framed thereunder.

In pursuance of above said circular and the provisions of the Act, 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.

1. Initiatives

The basic purpose of the AML Policy is to establish a system for Aurum Capital Projects Limited to participate in the international efforts against ML and to duly comply with the guidelines as detailed in the above circular of SEBI, as amended and other legal provisions and to ensure that Aurum Capital Projects Limited is not used as a vehicle for ML. The AML framework of the company would meet the extant regulatory requirements.

2. Scope:

This AML Policy establishes the standards of AML compliance and is applicable to all activities of Aurum Capital Projects Limited.

3. Objectives of the Policy:

- i. To establish a framework for adopting appropriate AML Procedures and controls in the operations / Business processes of Aurum Capital Projects Limited.
- 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 are adequately trained in KYC/AML procedures.
- v. To assist law enforcement agencies in their effort to investigate and track money launderers.

4. Principal Officer – Designation and Duties:

The company has designated the Company Secretary as the Principal Officer for due compliance of its AML measures. He 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 duties of the Principal Officer will include monitoring the company's compliance with AML obligation and overseeing maintenance of AML records, communication and training for employees. The Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU–IND). Principal Officer is authorized to issue additional circulars and advisories, to and seek information from the concerned

officials for due compliance of AML measures from time to time. The company has provided the FIU with contact information of the Principal Officer and will promptly notify FIU of any change in this information.

5. Customer Due Diligence:

At the time of opening an account the company will verify the identity records and current address(es) including permanent address(es) of the client, the nature of the business of the client and his/her financial status by scrupulously following the KYC norms. Adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship should be obtained. KYC norms shall be followed while establishing the client relationship and may further be followed while carrying out transactions for the client or when there is doubt regarding the veracity or adequacy of previously obtained client identification data.

Reliance would be placed on the documents as prescribed by the Securities and Exchange Board of India/Exchange for opening of Account as applicable from time to time. Account can be opened only after the completion of all the required documents and after due verification with originals. The concerned official of the company will put his signature with the stamp "verified with original" after due verification with the original documents on the copy thereof.

Additionally following norms shall be observed:

- i) No account will be opened in a fictitious, benami name or anonymous basis.
- ii) Adhering to parameters developed to enable classification of clients into low, medium, and high risk.
- iii) Documentation requirement and other information may be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of the Prevention of Money Laundering Act, 2002 and the guidelines issued by SEBI from time to time.
- iv) The company shall consult the relevant authority, in case return of securities or money that may be from suspicious trades is desired.
- v) Any person other than the constituent can operate the account of the constituent only if he/she has been duly authorized by the constituents. In case of body corporate or other entities, accounts can be operated only by the authorized persons supported by necessary documents. It is further clarified that the transaction limits for the operation, required margin and the trading relations with the clients will be governed as per the Circular, Rules, Regulations and Bye laws of SEBI/Exchange and as per agreement(s) with the constituents. It is further reiterated that all payments should be received by cheque and all payments should be made through cheque. Cash transactions are not allowed as per the direction of the SEBI/Exchange and the company shall comply with the same.
- vi) Before opening an account Company will ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide and may take declaration to this effect from the prospective client.

On failure by prospective client to provide satisfactory evidence of identity, new account shall not be opened and the matter shall be reported to the higher authority.

vii) No accounts will be opened without acceptance of a copy of PAN Card as directed by SEBI/Exchange. The said PAN received will be verified from the Income Tax/NSDL website before the account is opened.

viii) Without diluting the above requirements, the personnel opening a new account may obtain other independent information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

ix) Records of all identification information shall be maintained for ten years after the account has been closed unless some inquiry/investigation is pending at that time for which retention for further period is directed by an agency/authority. Special care shall be taken while opening accounts of Clients of Special Category (CSC). Such clients include the following:

a. Non-resident clients

b. High net worth clients

c. Trust, Charities, NGOs and organizations receiving donations

d. Companies having close family shareholdings or beneficial ownership

e. Politically exposed persons (PEP) of foreign origin e.g. current/former heads of states, current/former senior high profile politicians, senior government/ judicial/ military, senior executives of state-owned corporations and connected persons (immediate family, close advisors and companies in which such individuals have interest or significant influence)

f. Companies offering foreign exchange offerings.

g. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspected, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per transparency international corruption perception index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.)

h. Non-face to face clients

i. Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the company exercises independent judgment to ascertain whether new clients should be classified as CSC or not.

x) The Company shall duly comply with the KYC / client identification procedures that may be specified by SEBI from time to time.

xi) The concerned officials should take extra caution in case of existing or potential Politically Exposed Persons (PEP). They may seek additional information and also take the help of publicly available information.

xii) No business relationships can be established with PEP without the permission of any of the Directors of the Company or the Principal Officer. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, the approval from the above said officials is required to continue the business relationship.

xiii) The Officials of the Company may track the financial soundness of the clients and shall take reasonable measures to verify source of funds of clients identified as PEP.

6. Maintenance of records:

The Principal Officer shall ensure the maintenance of the following records:

- all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transaction have taken place within a month;
- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- all suspicious transactions - Suspicious transaction means a transaction whether or not made in cash and including inter-alia, credits or debits into or from any non-monetary account such as demat account, security account etc. which, to a person acting in good faith gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or appears to be made in circumstances of unusual or unjustified complexity; or appears to have no economic rationale or bonafide purpose.

The records shall contain the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

The Company shall also endeavour to maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence to the investigating agencies for prosecution of criminal behavior. For this purpose the company shall retain the documents as to:

- a) the beneficial owner of the account;
- b) the volume of the funds flowing through the account; and
- c) for selected transactions:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

The Principal Officer shall ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, he may consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

7. Retention of Records:

The records of the identity of clients is maintained and preserved for a period of ten years from the date of cessation of transactions between the client and the Company. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that case has been closed.

8. Monitoring Accounts for Suspicious Activity:

The following kinds of activities are to be treated as red flags and reported to the Principal Officer:

- i. Clients whose identity verification seems difficult or clients appear not to cooperate
- ii. Where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- iii. Clients in high-risk jurisdictions or clients introduced by such clients or banks or affiliates based in high risk jurisdictions;
- iv. Substantial increases in business without apparent cause;
- v. Unusually large cash deposits made by an individual or business;
- vi. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- vii. Transfer of investment proceeds to apparently unrelated third parties;
- viii. Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export/import of small items.

The above mentioned list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances.

When any functionary of the company detects any red flag, he or she will cause it to be further investigated for his/her satisfaction or report the same to the Principal Officer for further investigation and necessary action.

9. Reporting to Financial Intelligence Unit –India

In terms to the PMLA rules, Principal Officer is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).

For Cash Transaction Reporting :

Dealings in Cash, if any, requiring reporting to the FIU IND will be done in the STR format and in the manner and at intervals as prescribed by the FIU IND.

Procedure for Suspicious Transactions Reporting:

The staff at operating terminal shall be adequately trained with PMLA requirements and reporting suspicious transaction to Principal Officer .The Principal Officer will make a note of suspicion transaction that have not been explained to his satisfaction and thereafter report the same to the FIU IND within the required deadlines.

Where a client aborts/abandons a suspicious transaction on being asked some information by the company officials, the matter shall be reported to FIU in the STR irrespective of the amount by the Principal Officer. The Principal Officer will not base the decision on whether to file a STR solely on whether the transaction falls above a set threshold. The Principal Officer will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal or terrorist corrupt activities.

The Company will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PML A Act and Rules thereof.

Utmost confidentiality shall be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported. The Company shall not put any restrictions on operations in the accounts where an STR has been made. Aurum Capital Projects Limited and its directors, officers and employees (permanent and temporary) shall be prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. It should be ensured that there is no tipping off to the client at any level. The company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification and will maintain STRs and their accompanying documentation for such period as prescribed from time to time.

10. 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.

11. Confidential Reporting of AML Non-Compliance:

Employees report any violations of the company's AML compliance programme to the Principal Officer, unless the violations implicate the Principal Officer, in which case the employee shall report to the Managing Director. Such reports are confidential, and the employee suffers no victimization for making them.

12. 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.

13. Communication

Principal Officer shall ensure that this policy is communicated to all management and relevant staff including Directors, customers and all concerned.