ANTI-MONEY LAUNDERING POLICY

This policy has been formed in the light of 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 after making necessary amendments in the existing Anti-Money Laundering Policy of the Company.

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 by MST

The basic purpose of the AML Policy is to establish a system for MST to participate in the international efforts against ML (Money Laundering) and to duly comply with the guidelines as detailed under various requirements under law from time to time, as amended and other legal provisions and to ensure that MST is not used as a vehicle for ML. The AML framework of MST would meet the extant regulatory requirements.

2. Scope:

This AML Policy establishes the standards of AML compliance and is applicable to all activities of MST.

3. Objectives of the Policy:

1. To establish a framework for adopting appropriate AML Procedures and controls in the operations / Business processes of MST.
2. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
3. To comply with applicable laws and regulatory guidelines.
4. To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.
5. To assist law enforcement agencies in their effort to investigate and track money launderers.

4. Principal Officer – Designation and Duties:

The Compliance Officer shall act as a central reference point in facilitating onward reporting of suspicious transactions and 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 obligations and overseeing the maintenance of AML records, communication and training for employees. The Principal Officer will ensure the filing of necessary reports with the Financial Intelligence Unit (FIU–IND). The 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.

5. Customer Due Diligence:

At the time of opening an account, the company will verify the identity records and current address(es) including the permanent address(es) of the client, the nature of the business of the client and his 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.

The KYC norms will be conducted in accordance with the established KYC policies. This process encompasses Enhanced Customer Due Diligence for customers deemed as "High Risk." The determination of "High Risk" customers is solely at the discretion of MST.

Reliance would be placed on the documents as prescribed by various government authorities 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:

1. No account will be opened on a fictitious, benami name or anonymous basis.
2. Adhering to parameters developed to enable classification of clients into low, medium, and high risk.
3. Documentation requirements and other information may be collected with 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 various government authorities from time to time.
4. The company shall consult the relevant authority, in case the return of securities or money that may be from suspicious trades is desired.
5. 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 the case of body corporate or other entities, accounts can be operated only by authorized persons supported by necessary documents. It is further clarified that the transaction limits for the operation, required margin and trading relations with the clients will be governed as per the Circular, Rules, Regulations and Bye-laws 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 by cheque. Cash transactions are not allowed as per the direction of the any applicable government authority and the company shall comply with the same.
6. Before opening an account, Company will conduct a reasonable due-diligence which may include among others aspects a KYC compliance and a reasonable check on antecedents, whether in terms of criminal or civil proceedings by any enforcement agency worldwide and may take declaration to this affect from the prospective client.
7. On failure by a prospective client to provide satisfactory evidence of identity, new account shall not be opened and the matter shall be reported to the higher authority.
8. No accounts will be opened without acceptance of a copy of PAN Card as directed by any government authority.
9. 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.
10. 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:

1. Non-resident clients
2. High net worth clients
3. Trust, Charities, NGOs and organizations receiving donations
4. Companies having close family shareholdings or beneficial ownership
5. Politically exposed persons (PEP) of foreign origin e.g. current/former heads of state, 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.
6. Companies offering foreign exchange offerings.
7. Clients in high-risk countries (where the 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.)
8. 14. Non-face-to-face clients
9. Clients with dubious reputations 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. The Company shall duly comply with the KYC / client identification procedures that maybe specified by government authorities from time to time.

6. Transaction Monitoring & Reporting

MST shall implement blockchain analytics tools to track and flag suspicious transactions, including:

- Transactions with wallets linked to dark web activities.
- High-volume or frequent transactions from unknown or high-risk jurisdictions.
- Use of mixers, tumblers, or privacy-enhancing blockchain technologies.

Suspicious transactions identified shall be immediately reported to the FIU-IND in compliance with the Prevention of Money Laundering Act, 2002.

7. Prohibition on Transactions with Unregulated Virtual Asset Service Providers

MST shall not engage in transactions with unregulated virtual asset service providers, including unregistered crypto exchanges, decentralized finance (DeFi) protocols with no compliance mechanisms, and peer-to-peer (P2P) marketplaces that do not follow AML/KYC norms. MST shall verify that counterparties involved in transactions related to blockchain nodes are compliant with Indian and international AML regulations.

8. Restrictions on High-Risk Customers

MST reserves the right to refuse or restrict transactions in the following cases:

1. If a customer is flagged under global sanctions lists**,** such as those issued by the Financial Action Task Force , the Reserve Bank of India, or the Ministry of Home Affairs **.**
2. If the customer is associated with anonymous transactions**,** such as through privacy coins (e.g., Monero, Zcash) or anonymous wallets**.**
3. If the source of funds cannot be adequately verified or is linked to shell companies **or** unregistered investment schemes**.**
4. If the customer has been previously flagged under Suspicious Transaction Reports (STRs)**.**

9. Restrictions on Cash Transactions and Third-Party Payments

MST shall strictly prohibit the acceptance of cash payments for blockchain node sales. All transactions must be conducted through banking channels, including NEFT, RTGS, UPI, or other traceable payment methods. MST shall not accept payments from third parties who are not the direct buyer. All transactions must originate from an account held in the name of the customer undergoing KYC verification.

10. Record-Keeping Obligations for Virtual Asset Related Transactions

MST shall maintain transaction records, including KYC documentation and blockchain transaction logs, for at least ten (10) years after an account is closed or a transaction is completed. Blockchain node transaction records shall include:

- Wallet addresses of sender and recipient.
- Transaction hash and confirmation records.
- IP address logs for customer login and transaction execution.
- All communications related to KYC and transaction verification.

If required by any law enforcement agency, FIU-IND, or RBI**,** MST shall provide transaction details, even if customer accounts are no longer active.

11. Sanctions Compliance and Prohibited Jurisdictions

MST shall comply with sanctions imposed by the United Nations Security Council (UNSC), FATF, RBI, and the Ministry of Finance**.** Customers from sanctioned jurisdictions shall not be allowed to purchase blockchain nodes. The following jurisdictions are classified as high-risk and prohibited for transactions:

1. Countries blacklisted by FATF**.**
2. Countries facing economic sanctions by the Government of India or international regulatory bodies.
3. Any jurisdiction that does not comply with international AML/KYC regulations.

12. Reporting Obligations to FIU-IND

MST shall file the following reports with FIU-IND**:**

1 Transactions suspected to be linked to illicit activities.
2 Cash transactions exceeding INR 10 lakhs within a single month.
3 Transactions involving cross-border payments exceeding INR 5 lakhs.

If MST identifies any transaction involving potential terror financing or money laundering**,** it shall immediately notify FIU-IND and RBI**.**

13. Non-Compliance and Penalties

Any MST employee or customer found violating the AML policy shall be subject to immediate termination of services. MST reserves the right to report any non-compliant customer **to** law enforcement agencies and financial regulators**.** Penalties for non-compliance shall be determined in accordance with the Prevention of Money Laundering Act, 2002**,** and other applicable laws.

14. Maintenance of records:

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

1. All cash transactions of the value as time to time decided upon by MST in accordance with government regulations.
2. 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;
3. 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;
4. 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:

1. The nature of the transactions;
2. The amount of the transaction and the currency in which it was denominated;
3. The date on which the transaction was conducted; and
4. 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 the prosecution of criminal behaviour. For this purpose, the company shall retain the following documents as to:

1. the beneficial owner of the account;
2. the volume of the funds flowing through the account; and
3. for selected transactions:
4. The parties to the transaction.
    - . 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 laws, Rules and Regulations framed there under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

15. Retention of Records:

The records of the identity of clients is maintained and preserved for a period of five(5) years from the date of cessation of transactions between the client and the Company. In situations where the records relate to ongoing investigations or transactions which have been the subject of suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

16. Monitoring Accounts for Suspicious Activity:

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

1. Clients whose identity verification seems difficult, or clients who appear not to cooperate
2. Where the source of the funds is not clear or not in keeping with client's apparent standing business activity
3. Clients in high-risk jurisdictions or clients introduced by such clients or banks or affiliates based in high-risk jurisdictions;
4. Substantial increases in business without apparent cause;
5. Unusually large cash deposits made by an individual or business;
6. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
7. Transfer of investment proceeds to apparently unrelated third parties;
8. Unusual transactions by Client of Special Categories (HNI's, UHNI's, Foreign Nationals, NRI's or any other) 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.

17. 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.

18. Employee's Hiring /Employee's Training / Investor Education:

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. The implementation of AML measures requires intermediaries to demand certain information from investors which may be of personal nature or which have hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. Therefore, the Principal Officer and other officials of the company will sensitize the customers about these requirements as the ones emanating from AML framework so as to educate the customer of the objectives of the AML program.

19. Monitoring Employee Conduct and Accounts:

MST subjects employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. The Principal Officer's account is reviewed by the Managing Director.

20. Confidential Reporting of AML Non-Compliance:

Employees report any violations of the company's AML compliance program 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.

21. 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.

22. Communication

Principal Officer shall ensure that this policy is communicated to all management and relevant staff including Directors, Head of the Department (s), customers and all concerned.