PMLA POLICY

KNOW YOUR CLIENTS GUIDELINES & ANTI MONEY LAUNDERING STANDARDS

1. **INTRODUCTION:**

The Prevention of Money Laundering Act, 2002 and the rules made hereunder imposed an obligation on Banks/Financial institutions/Intermediaries/Registrars under SEBI Act, 1992 to verify the identity of clients, maintenance of records and furnishing information to Director, FIU-IND. Intermediaries defined under section 12 of SEBI Act, 1992 includes stock broker and sub broker/authorised persons also and Vijayranga Enterprises & Intermediaries (P) Limited being a stock broker needs to adhere to the same, thus PMLA Act becomes applicable to our Company.

It is policy of our Company to prohibit any activity and combating Money Laundering (ML) and Terrorist Financing (TF) that facilitates money laundering or funding of terrorism and criminal activities. The Company also exercises clients due diligence and define and segregate clients as special category in accordance to their risk profile.

The Company's money laundering policy is to combat Money Laundering (ML)and Terrorist Financing (TF) and identify and report any suspicious activity to Regulatory bodies.

The policies and guidelines are reviewed and updated as per applicable amendments and the same are conveyed through notices and meetings. The Company trains and educates the Employees/Clients/APs regarding Prevention of Money Laundering under various training programmes.

2. **Obligation to establish policies and procedures**

I. The PMLA is in line with these measures and mandates that all intermediaries ensure the fulfillment of the objectives.

II. To be in compliance with these obligations, the senior management of a registered intermediary is fully committed to establishing appropriate policies and procedures for the prevention of money laundering (ML) and terror funding (TF) and ensuring the ireffectiveness and compliance with all relevant legal and regulatory requirements. The Company shall:

a. issue a statement of policies and procedures, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
b. ensure that the content of these Directives are understood by all staff members;
c. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;
d. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
e. Undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
f. Have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
g. Develop staff members' awareness and vigilance to guard against ML and TF

3. <u>Policies and procedures to combat ML and TF shall cover:</u>

a. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
b. Client acceptance policy and client due diligence measures, including requirements for proper identification;
c. Maintenance of records;
d. Compliance with relevant statutory and regulatory requirements;
e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
f. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, 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; and,
g. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

4. <u>Written Anti Money Laundering Procedures</u>

The Company hereby adopting these written procedures to implement the anti money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following three specific parameters which are related to the overall 'Client Due Diligence Process.

Policy for acceptance of clients;

1. Procedure for identifying the clients;
2. Risk Management;
3. Monitoring of Transactions.

5. KNOW YOUR CLIENT STANDARDS

1. The objective of the KYC guidelines is to prevent sub-brokers/officials of the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable sub-brokers/officials of the Company to know / understand their clients and their financial dealings better, which in turn help them manage their risks prudently. The KYC policy of the Company incorporates the following elements:

   - Client document scrutiny
   - Clients due diligence (CDD)
   - Know your Client and Client Acceptance Policy (CAP)
   - Client Identification Procedures (CIP)
   - Monitoring of Transactions; and
   - Risk Management

2. A Client for the purpose of KYC Policy is defined as a person or entity that maintains an account and/or has a business relationship with any of our activities including Trading, Demat, Registrar, Share Transfer and Mutual Funds etc.

6. CLIENT DOCUMENT SCRUTINY

- No account shall be opened in anonymous or fictitious / benami name(s).

- Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of client and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of clients into low, medium and high risk called Level I, Level II and Level III respectively; Clients requiring very high level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as Level IV.

- The sub-brokers/officials shall collect documents and other information from the client depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by SEBI from time to time.

- The Authorised Person/officials shall close an existing account or shall not open a new account where it is unable to apply appropriate client due diligence measures i.e., Authorised Person/

officials are unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the client or non reliability of data/information furnished to the Company. The Authorised Person/officials shall, however, ensure that these measures do not lead to the harassment to the clients. However, in case the account is required to be closed on these grounds, they shall do so only after permission of the Chief Executive Officer and or the Whole Time Director of the Company is obtained. Further, the client should be given a prior notice of at least 30 days, wherein reasons for closure of his account should also be mentioned. The Authorised Person/officials shall make necessary checks before opening a new account so as to ensure that the identity of the client does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. SEBI has been circulating lists of terrorist entities notified by the Government of India so that brokers exercise caution against any transaction detected with such entities. The Officials shall invariably verify such lists to ensure that prospective person/s or organizations desirous to establish relationship with the Company are not in any way involved in any unlawful activity and that they do not appear in such lists.

- The sub-brokers/officials shall prepare a profile for each new client based on risk categorization. The Company has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new client. The forms are separate for Individuals, Partnership Firms, Corporate and other legal entities, etc. The nature and extent of due diligence shall depend on the risk perceived by the Sub broker/officials. The APs/officials should continue to follow strictly the instructions issued by the Company regarding secrecy of client information. The officials of the Company should bear in mind that the adoption of client document scrutiny policy and its implementation does not become too restrictive.

7. CLIENT DUE DILIGENCE (CDD)

The CDD measures comprise the following:

i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;

ii. Verify the client's identity using reliable, independent source documents, data or information;

iii. Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted -

a) **For clients other than individuals or trusts:** Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals,

the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

aa) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means owner-ship of/entitlement to:
i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.
bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means;

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.
cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

b) **For client which is a trust:** Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the author of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership;
c) **Exemption in case of listed companies:** Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies;

d) **Applicability for foreign investors**: Registered intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client;

e) The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

iv. Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (iii);

v. Understand the ownership and control structure of the client;

vi. Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;

vii. Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data; and

viii. Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

8. Policy for acceptance of clients

All registered intermediaries shall develop client acceptance policies and procedures that aim to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, they will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards are to be followed while accepting the clients:

i. No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified;

ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile;

iii. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

a) Non- resident clients;

b) High net-worth clients;

c) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations;
d) Companies having close family share holdings or beneficial ownership;

e) Politically Exposed Persons (PEP). PEP are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The additional norms applicable to PEP as contained in the subsequent paragraph 14 of this circular shall also be applied to the accounts of the family members or close relatives of PEPs;

f) Clients in high risk countries. While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas;

g) Non face to face clients. Non face to face clients means clients who open accounts without visiting the branch/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients;

h) Clients with dubious reputation as per public information available etc; The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

i) Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

v. Ensure that an account is not opened where the intermediary is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non - co-operation of the client in providing full and complete information. The registered intermediary shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. The registered intermediary shall be cautious to ensure that it does not return securities or money that may be from suspicious trades. However, the registered intermediary shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

vi. The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons i.e. the agent- client registered with the intermediary, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

vii. Necessary checks and balance to be put into place before opening an account so as to 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.
viii. The CDD process shall necessarily be revisited when there are suspicions of ML/TF.

9. Client identification procedure:

1. The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data. We should be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

(a) We shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.

(b) It is required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, company shall required to obtain senior management approval to continue the business relationship.

(c) It shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP".

(d) The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

(e) The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.

(f) Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

2. SEBI has prescribed the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time as detailed in the table. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, the Company shall follow the procedure as direction given by the Principal Officer in this manner based on experience in dealing with their clients and legal requirements as per the established practices. Further, we conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that the intermediary is aware of the clients on whose behalf it is dealing.

3. The CIP shall be hereby adopted and implemented which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the Company and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients. We shall also adhere to the amended rules of PML vide notification No. 13/2009 dated November 12, 2009.

4. We shall obtain the minimum information/documents from clients as stipulated in the PML Rules/SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients irrespective of the amount of investment made by clients. Further no exemption from carrying out CDD exists in respect to fancy category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by the Company.

- If Authorised Person / officials need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new client, whether regular or occasional, and the purpose of the intended nature of brokering/other financial services relationship. Being satisfied means that The Authorised Person, officials are able to satisfy the competent authorities that due diligence was observed based on the risk profile of the client in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of client (individual, corporate, etc). For clients that are natural persons, The Authorised Person, officials shall obtain sufficient identification data to verify the identity of the client, his address / location, and also his recent photograph. For clients that are legal persons or entities, The Authorised Person, officials shall
- (i) verify the legal status of the legal person/entity through proper and relevant documents

- (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person
  (iii) understand the ownership and control structure of the client and determine who are the natural persons who ultimately control the legal person. Client Identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution.

- If Authorised Person, officials decide to accept such accounts in terms of the Client Acceptance Policy, he or she shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner is/are. An indicative list of the nature and type of documents/information that may be relied upon for client identification.

The Client Identification Procedure (CIP) includes that clients should be classified as per their risk profile and the risk to the client shall be assigned on the following basis:

- **Low Risk (Level I):**

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Also who makes payment/delivery in time and follow the norms established by regulators and Company. The illustrative examples of low risk clients could be salaried employees, whose salary structures are well defined, people belonging to lower economic strata of the society, whose accounts show small balances and low turnover, Government Departments and Government owned companies, Regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the client shall be met.

- **Medium Risk (Level II):**

Clients that are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on client's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

• Persons in business/industry or trading activity where the area of his residence or place of business has scope or history of unlawful trading/business activity. • Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious. • Clients who deal in intraday speculative transactions and whose turnover is not in line with financials declared.

- **High Risk (Level III):**

The sub brokers/authorised persons/officials of the Company may apply enhanced due diligence measures based on the risk assessment, there by requiring intensive 'due diligence' for higherrisk

clients, especially those for whom the sources of funds are not clear. The examples of clients requiring higher due diligence may include:

a) Non Resident Clients,
b) High Net worth individuals with an annual income of Rs.50 lakhs and above and in case of non-individual clients having more than Rs.2 Crores as income or with a Net worth of more than Rs.50 Crores.
c) Trusts, Charities, NGOs and organizations receiving donations,
d) Companies having close family share holding or beneficial ownership
e) Firms with 'sleeping partners'
f) Politically Exposed Persons (PEPs) of foreign origin
g) Those with dubious reputation as per public information available, etc. having criminal backgrounds
h) Clients having multiple accounts.

The persons requiting very high level of monitoring are categorized as **Level IV**.
The records evidencing the identity of the clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between the client and the Company has been ended or the account has been closed.

10. CLIENTS OF SPECIAL CATEGORY (CSC):

Vijayranga Enterprises & Intermediaries (P) Limited will always identify clients of special category which includes NRI, High Net worth Clients, Trusts, Charities, Non-Government Organization, Companies having close family share holdings, Politically exposed persons, Companies offering foreign exchange offering, Clients residing in high risk countries or countries active in narcotics productions, etc, Non face to face clients and clients with dubious reputation as per public information available. High level client due diligence will be undertaken for CSC

11. MONITORING OF TRANSACTIONS

- Continuous monitoring is an essential ingredient of effective AML procedures and the extent of monitoring should be according to the risk sensitivity of the account. Authorised Person /officials shall pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Transactions that involve large amount of cash inconsistent with the size of the balance maintained may indicate that the funds are being ‘washed’ through the account. High risk accounts shall be subjected to intensive monitoring.

- The present responsibility of monitoring are with the APs and key officials of the Company, Company Secretary and Compliance Officer and also with the Chief Executive Officer and

Also Whole Time Director, who are appointed as the Designated Director/Supervisor to Principal Officer for AML implementation.

- The Central account processing services, Secretarial and Compliance Department shall ensure adherence to the KYC policies and procedures. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses, if any observed in this regard. 'The compliance in this regard shall be put up before the Chief Executive Officer and or Whole Time Director, All staff members shall be provided training on Anti Money Laundering, The focus of training shall be different for frontline staff, compliance staff and staff dealing with new clients.

- The Company shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

- Further, the compliance cell of the Company shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

- The Company shall maintain and preserve the record of information related to transactions that are monitored for a period of five years from the date of transaction between the client and the Company.

12. SUSPICIOUS TRANSACTIONS:

a) Identification:-

"Suspicious transaction" means a transaction whether or not made in cash, which to a person acting in good faith-

- gives rise to a reasonable ground of suspicion that it may involve proceeds of an Offence specified in the Schedule to the Act, regardless of the value involved; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; of
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;
- Clients based in high risk jurisdiction.
- Substantial increase in business without apparent cause.
- Transactions reflect likely market manipulations.
- Sudden activity in dormant accounts.
- Clients whose identity verification seems difficult or clients that appear not to cooperate;
- Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
- Clients based in high risk jurisdictions;

- Substantial increases in business without apparent cause;
- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- Attempted transfer of investment proceeds to apparently unrelated third parties;
- Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.
- Any suspicious transaction shall be immediately notified to the Designated/Principal Officer within the Company. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.
- It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that registered intermediaries shall report all such at tempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction

b) Reporting of suspicious transaction:

The Principal Officer shall report the nature, amount, date and all related details of any and all the suspicious transactions recorded to the Director, Financial Intelligence Unit – India situated at New Delhi as per the format enclosed for the reporting. The Principal Officer shall maintain and preserve the record of transactions reported to the Director, Financial Intelligence Unit — India, for a period of five years from the date of transaction between the client and the Company.

c) Supplemental Guidelines for Detecting suspicious transactions under rule 7(3) of prevention of Money Laundering (Maintenance of Records) Rules, 2005:

Indicative Alert Indicators

Sr. No.	Alert Source	Alert Indicator	Indicative Rule/ Scenario
1	Transaction Monitoring	TM 11 - Fund Received from Non-Clients	Single or multiple transfer of funds more than 1Cr in a calendar month in broken account from multiple sources/accounts which are not reported As clients
2	Transaction Monitoring	TM 12 - Margin Trading	Sudden Increase in the funding amount of Margin Trading Facility (MTF) exposure

			1. By more than 50% of MTF exposure of previous month AND; 2. with a value of more than Rs. 10 crores.
3	Transaction Monitoring	TM 13 - Off Market transfer to unrelated accounts (Refer Note No. 1)	1. Only for Reason code/s - off – market sale - Gift - Donation AND; 2. Valuation per debit transaction will be > 25 lacs AND; 3. Exclude accounts with same PAN, mobile, email ID, same bank details (IFSC + ac no) (same mobile / email / bank details in multiple demat account will be treated as related accounts) and family flag is enabled AND; 4. Valuation is >5times of income range
4	Transaction Monitoring	TM 13A - Suspicious Off Market Credit and Debit [Refer Note No. 1]	Customer receive credit / demat of 50,000 shares or shares worth Rs. 25 lakhs and above by single transaction or series of transactions in an ISIN AND; 2. 80% or more of credited shares gets debited by way Off Market transfers to 3 or more than 3 unrelated accounts AND; 3. Only Listed Equity Shares will be considered for this alert. (Monthly frequency) Short span of time is within 30 days.
5	Transaction Monitoring	TM 13B - Off market delivery in unlisted scrip [Refer Note No. 1]	1. Single or Series of Transactions where more than 5,00,000 unlisted equity shares have been transferred within period of 1 month AND; 2. Off-Market Transfers with Reason code "Off-Market Sale", "Donation" and "Gift" will be considered AND; 3. Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer To own accounts. (Monthly frequency)

6	Transaction Monitoring	TM 13C - Gift, Donation related off-market transfer (Refer Note No.1)	1. Transaction value of such transaction is beyond 5 times of Income range/Net worth (as updated in demat account) on higher side as provided by the BO AND; 2. Listed Equity Shares will be considered AND; 3. Debit transaction specific reason codes > 5 lacs in value AND; 4. For Reason code's - Family Account Transfer - Gift - Donation
7	Transaction Monitoring	TM 13D - Off Market transfer at variance with market value (Refer Note No. 1]	1. Off market transfers with reason code 'Off-Market Sale" AND; 2. Difference of +/- 50% difference in consideration value mentioned by BO and prevailing market value of Equity Shares AND; 3. Only Listed Equity Shares will be considered. AND; 4. Minimum transaction value for alert will be Its 251akhs AND;
8	Transaction Monitoring	TM 13E - Off Market transfer in suspicious scrip (Refer Note No. 1)	1. Off market single or series of transactions having value of Rs 2 lakh and above AND; 2. Suspicious Scrips for which unsolicited SMSs were circulated will be taken from below URLs BSE https://www.bseindia.com/attention_investors.aspxN SE: https://www.nseindia.com/regulations/unsolicited-messages-report

9	Employee Initiated	EI 13 - Suspicious Closure of Account (Refer Note No. 1)	1. Accounts closed within 30 days of opening of Account and single or series of debit transactions (On Market, Off-Market including IDT Transfer) with value > 10 lacs AND; 2. Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer to own accounts. Also, if securities received in Source account through transmission, then the
			Same will be excluded

Note No. 1: Alerts in respect of TM 13, TM 13A TM 13B, TM 13C, TM 13D, TM 13E & EI 13 indicators will also be generated

13. Reporting to Financial Intelligence Unit - India

I. In terms of the PML Rules, Company are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit- India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi - 110001,
INDIA Telephone: 91-11-23314429,
23314459
91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in
(For FIN net and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity/Principal Officer registration related queries)
complaints@fiuindia.gov.in
Website: http://fiuindia.gov.in

II. Company shall carefully go through all the reporting requirements and formats that are available on the website of FIU –IND under the Section Obligation of Reporting Entity – Furnishing Information - Reporting Format (https://fiuindia.gov.in/files/downloads/ Filing_Information.html). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND.

III. The related hardware and technical requirement for preparing reports, the related data files and data structures there of are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, registered intermediaries shall adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.

iii. The Non Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month.

iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.

vi. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.

Company shall not put any restrictions on operations in the accounts where an STR has been made. Company and their 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. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.
It is clarified that the Company, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified
in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.
It is further clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

14. Information to be maintained

The Company is required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

i. The nature of the transactions;

ii. The amount of the transaction and the currency in which it is denominated;

iii. The date on which the transaction was conducted; and

iv. The parties to the transaction

d) Record Keeping

Vijayranga Enterprises & Intermediaries (P) Limited will comply with all requirements of record keeping under SEBI Act 1992, rules regulation made under PMLA as well as other legislations, rules and regulation, Exchange's bye laws and circulars. More specifically Vijayranga Enterprises & Intermediaries (P) Limited will maintain records of all the transactions prescribed under mules 3 of PML Rules for a period of five years.

- The Company shall 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 for prosecution of criminal behaviour.

- In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, The Company shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

i. The beneficial owner of the account;
ii. The volume of the funds flowing through the account; and
iii. For selected transactions:

a. The origin of the funds
b. The form in which the funds were offered or with drawn, e.g. cheques, demand drafts etc.
c. The identity of the person undertaking the transaction;
d. The destination of the funds;
e. The form of instruction and authority.

- The Company shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

- The Company shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

ii. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency; It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from ‘transactions integrally connected’, ‘transactions remotely connected or related’ shall also be considered.

iii. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any for gery of a valuable security or a document has taken place facilitating the transactions;

iv. all suspicious transactions 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 maintained by the registered intermediary.

15. Retention of Records

- The Company shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.

- The Company are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, which ever is later.

- In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

- The Company shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

16. RISK MANAGEMENT

- The KYC policies and procedures of the Company covers management oversight, systems and controls, segregation of duties, training and other related matters. For ensuring effective implementation of the Company's KYC policies and procedures, the officials shall explicitly allocate responsibilities within the branch. The sub broker 'officials shall prepare risk profiles of all their existing and new clients and apply Anti Money Laundering measures keeping in view the risks involved in a transaction, account or brokering/business relationship.

- Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the Company's policies and procedures to combat money laundering shall be provided to all the staff members of the broker periodically in phases.

- The Management prescribes threshold limits of Rs. 5 Crores for level IV clients and The Sub broker/APs, officials shall pay particular attention to the transactions, which exceed these limits, The threshold limits shall be reviewed annually and changes, if any, conveyed to Sub broker/APs, officials for monitoring.

- The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, the registered intermediaries shall monitor the implementation of the controls and enhance them if necessary.

- It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

  - Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

17. Risk Assessment

a. The Company shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

b. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

c. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

18. EDUCATION

A) Employees' Training and Investor Education

Vijayranga Enterprises & Intermediaries (P) Limited has the policy for the ongoing training of the employees of Vijayranga Enterprises & Intermediaries (P) Limited at least once in 6 months or earlier covering the front line staff, back office staff, compliance staff, risk management staff, and staff dealing with the new clients. The Company also take care that all the concerned staff are well equipped with the objectives, obligations and requirements of the act and risk involved in it. The Principal Officer and the Compliance Officer are the key persons to educate the above at least once in 6 months to the staffs of Vijayranga Enterprises & Intermediaries (P) Limited.

B) SubBroker/Clients/Authorized Person Education

It is very important for our Organization to impart the education to our investors as well and also to get certain information from investors, which includes documents evidencing source of funds / income tax/ bank records etc. Therefore training programs are also organized for the investors.

C) Hiring of Employees:

The registered intermediaries shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

19. NEW TECHNOLOGIES

The KYC procedures shall invariably be applied to new Technologies to such other product, which may be introduced by the Company and take measures, if needed to use in money laundering schemes.

Sub broker/APs, officials should ensure that appropriate KYC procedures are duly applied before issuing the client code to the clients.

While, the guidelines shall apply to all new clients/accounts, Sub broker/APs, officials shall apply these to the existing clients on the basis of materiality and risk. However, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Client Due Diligence (CDD) measures. It is however to be ensured that all the existing accounts of companies, firm, trusts, charitable, religious organizations and other institutions are subjected to KYC standards, which would establish the identity of the natural/legal person and those of the 'beneficial owners'.

20. RESPONSIBILITIES OF DESIGNATED DIRECTOR/PRINCIPAL OFFICER

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the Company, Chief Executive Officer and or Whole Time Director shall act as Supervisor to Principal Officer cum Designated Director. He/she shall be responsible to monitor and report transactions and share information on Anti Money Laundering as required under the law. The Principal Officer shall

maintain close liaison with enforcement agencies, brokers and any other institutions that are involved in the fight against money laundering and combating financing of terrorism.

Annexure-I

Client Identification Requirements - Indicative Guidelines

Particulars	Guidelines
Trust/Nominee or Fiduciary Accounts	There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the client identification procedures. The Sub broker/APs, officials should determine whether the client is acting on behalf of another person as trustee / nominee or any other intermediary. If so Sub broker/AP, officials shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, Sub broker/APs, officials should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the Founder managers/directors and the beneficiaries, if defined.
Accounts of companies and firms	Sub broker/APs, officials need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with Company. Sub broker/APs, officials should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g, in the case of a public Company it will not be necessary to identify all the share holders. But at least promoters, Directors and its executives need to be identified adequately.
Client accounts opened by professional intermediaries	When The Sub broker/APs, officials have knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Sub broker/officials may hold 'pooled' accounts managed by professional intermediaries on behalf of Entities like mutual funds, pension funds or other types of funds. Sub broker/ APs, officials should also maintain 'pooled' accounts managed by Lawyers/Chartered Accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the Intermediaries are not co-mingled at the branch and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such accounts are co-mingled at the branch, the branch should still look through to the beneficial owners. Where the broker rely on the 'client due diligence' (CDD) done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems In place to comply with the KYC requirements.
Accounts of Politically	Politically exposed persons are individuals who are or have been

Exposed Persons (PEPs) resident outside India	entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Sub broker/ APs, officials should gather sufficient information on any person/client of this category intending to establish a relationship and check all the information available on the person in the public domain. Sub broker/ APs, officials should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a client. The Sub broker/APs, officials should seek prior approval of their concerned Heads for opening an account in the name of PEP.
Accounts of non-face-to-face clients	With the introduction of telephone and electronic brokering, increasingly accounts are being opened by brokers for clients without the need for the client to visit the broker branch. In the case of non-face-to-face clients, apart from applying the usual client identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents may be called for. In such cases, The Sub broker/APs, officials may also require the first payment to be effected through the client's account if any with another broker, which, in turn, adheres to similar standards. In the case of cross-border clients, there is the additional difficulty of matching the client with the documentation and the Sub broker /officials might have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has Adequate KYC systems in place.

Name Of the Company: Vijayranga Enterprises & Intermediaries (P)Limited

FIU-Registration Number:

Designated Director: Shamasastry Nagarathna Ravi

Principal Officer: Naina Poghul

Annexure-II

Client Identification Procedure

Features to be verified and documents that May be obtained from Clients

Features Documents

Accounts of Individuals	❖ Legal name and any other names used ❖ Correct permanent address (i)Passport (ii) PAN Card Voter's Identity Card (iii) Driving License (iv)Identity Card (subject to the satisfaction of the branch) (v) Letter from a recognized public authority or public servant verifying the identity and residence of the client to the satisfaction of branch (vi) Telephone bill (vii) Broker account statement (viii) Letter from any recognized public authority (ix)Telephone Bill (x) (xi) Electricity Bill (xii) Ration Card (xiii) Letter from the employer, (subject to the satisfaction of the branch) (xiv) Any other document, which Provides client in formation to The satisfaction of the broker will suffice.
Accounts of Companies	❖ Name of the Company ❖ Principal place of Business ❖ Mailing address of the Company ❖ Telephone/Fax Number i. Certificate of Incorporation and Memorandum & Articles of Association ii. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account iii. Power of Attorney granted to its managers, officers or employees to transact business on its behalf iv. Copy of PAN allotment letter v. Copy of the telephone bill

Accounts of Partnership Firms	❖ Legal name ❖ Address ❖ Names of all partners and their addresses ❖ Telephone numbers of the firm and partners (i) Registration certificate, if registered (ii) Partnership deed
	(iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts &Foundations	❖ Names of ❖ trustees, settlers, beneficiaries and signatories ❖ Names and addresses of the founder, the managers /directors and the beneficiaries ❖ Telephone/Fax numbers i. Certificate of registration, if registered ii. Power of Attorney granted to transact business on its behalf iii. Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/ managers / directors and their addresses iv. Resolution of the managing body of the foundation/association v. Telephone bill

Name Of the Company: Vijayranga Enterprises & Intermediaries (P) Limited

FIU-Registration Number:

Designated Director: Shamasastry Nagarathna Ravi

Principal Officer: Naina Poghul

POLICYONCONFLICTOFINTEREST

Internal Policy on Conflict of Interest

Vijayranga Enterprises & Intermediaries (P) Limited (hereinafter "the Company") which is engaged in providing financial services in Indian Capital Markets to retail investors and high networth individuals. The Company is registered as a Stock Broker with the Bombay Stock Exchange India Limited. The Company is also a SEBI registered Depository Participant of NSDL.

SEBI, vide its circular no. CIR/MIRSD/5/2013 dated August 27, 2013 has laid down the guidelines requiring registered intermediaries to establish and implement a conflicts of interest policy (herein after the "Policy").

To adhere to the above guidelines, the Company is required to take all reasonable steps to identify, eliminate or manage conflicts of interest. The Company is committed to acting honestly, fairly and professionally and in the best interests of its clients.

This Policy is not intended to, or does not create third party rights or duties nor does it form part of any contract between the Company and any client.

As the Company does not trade on its proprietary account presently and all the orders are passed to the market (no internal matching), chances of conflict of interest are minimized. Further, the Company is not having Sales/Marketing/Research wings/departments presently and hence chances of conflict of interest are minimized.

Purpose

The purpose of this Policy is to set out the Company's approach to identify and manage conflicts of interest, which may arise during the course of its business activities.

This Policy aims at:

a. Identifying circumstances which may give rise to conflicts of interest entailing a material risk of damage to clients' interests,
b. Establishing appropriate procedures and systems to manage those conflicts, and
c. Ensuring the maintenance of such procedures and systems in an effort to prevent actual damage to clients' interests through conflicts identified.

Scope

The Policy applies to the Board of Directors and Employees of the Company (collectively referred to as 'Stakeholder) and relevant sub brokers/authorized persons/associated persons as defined in SEBI (Certification of associated persons in the securities market) Regulations,

2007 with respect to all interactions with the clients.

Potential **conflicts of interest** areas

1. The Company or employees or relevant associated person(s) is/ are likely to make a financial gain, or avoid a financial loss, at the expense of the client.

2. The Company or employees or relevant associated persons has/have an interest in the outcome of a service provided to the client or of a transaction carried out on behalf of the client, which is distinct from the client's interest in the outcome.

3. The Company or employees or relevant associated person(s) has/have a financial or other incentive to favor the interest of another client or group of clients over the interest of one client.

4. The Company or employees or relevant associated persons receives or will receive from a person other than the client an inducement in relation to a service provided to the client, in the form of monies, goods or services, other than the standard commission or fee for that service.

Procedures and controls to managing Conflicts of Interests

The procedures and controls that the Company follows to manage the identified conflicts of interests include the following:

1. Effective procedures to prevent or control the exchange of information in the activities involving a risk of conflict of interest where the exchange of that information is likely to harm the interest of one or more clients;

2. Measures to prevent or limit any person from exercising in appropriate influence over the way in which capital market services are carried out;

3. Chinese walls restricting flow of confidential and price sensitive information within the Company, physical separation of departments and sharing of information only on a "Need to Know Basis". The same shall be governed by 'Prevention of Insider Trading Policy' applicable to the Company. The purpose is to set out the Company's approach to prevent the misuse of confidential information. In this regard, the Company shall adopt a "Chinese Wall" policy which separates those areas of the Company which routinely have access to confidential information, considered "inside areas" from those are as which deal with

sale/marketing/investment advice or other departments providing support services, considered "public areas" during the course of its business activities. Even though the Company is not having any Sales/Marketing/ Investment Advise wings presently, this policy is formulated to take care of its future requirements, in case these wings/departments are created in future.

In order to achieve the above purpose, the Company shall ensure that:

a) The employees in the inside area shall not communicate any Price Sensitive Information to anyone in public area.
b) The employees in inside area maybe physically segregated from employees in public area.
c) Demarcation of the various departments as inside area shall be implemented by the Company as and when it is needed.

d) In exceptional circumstances employees from the public areas may be brought *"over* the wall" and given confidential information on the basis of "need to know" criteria, under intimation to the Compliance Officer.
e) Employees shall maintain the confidentiality of all Price Sensitive Information. Employees shall not pass on such information directly or indirectly by way of making are commendation for the purchase or sale of securities.
f) Price Sensitive information shall be handled on a "need to know" basis, i.e. Price Sensitive Information shall be disclosed only to those within the Company, who need the information to discharge their duty and whose possession of such information will not give rise to a conflict of interest or appearance of misuse of the information.
g) Files containing confidential information shall be kept secure.
h) Computer files shall have adequate security of login and password, etc.

Procedures and controls to ensure compliance to the Policy

a. The Company's Compliance team shall have oversight on the business to ensure that internal controls are appropriate in this regard.
b. Chinese walls restricting flow of confidential and price sensitive information within the Company, physical separation of departments and sharing of information only on a “Need to Know Basis” shall be ensured.

4. Measures to limit the conflicts of interests arising from the giving and receiving of inducement.

5. Appointment of Independent Internal auditors to ensure that appropriate

systems and controls are maintained and their effectiveness or otherwise

Is being reported to the Company's Board of Directors.

6 Personal account dealing requirements applicable to employees in relation to their own investments needs an approval from the Compliance Team by submission of an Investment Request Form. The same shall be governed by ‘Prevention of Insider Trading Policy' applicable to the Company.

7. The employees are governed by measures laid down in the internal code of conduct and other policies, which include the following:
   a. restrictions on dealing in securities while handling client's mandate or while in possession of material non published information, or communicating such information while dealing on client's behalf, manipulating demand or supply of securities or influencing their market price. The same shall be governed by ’Prevention of Insider Trading Policy' applicable to the Company.
   b. Restrictions on an incentive structure that encourages sale of products not suiting the client's risk profile.
   c. Restrictions on divulgence of client's confidentiality unless required by or under the law.
   d. The sub brokers/authorized persons/associated persons shall at all times maintain high standards of integrity in the conduct of their business followed by compliance reporting to Board of Directors and the Senior Management.
   e. Ensure fair treatment of their clients and not discriminate amongst them.
   f. Ensure that their personal interest does not, at anytime conflict with their duty to their clients and client's interest always takes primacy in their advice, investment_ decisions and transactions;
   Make appropriate disclosure to the clients of possible source or potential areas of conflict of interest, which would impair their ability to render fair, objective and unbiased services;
   g. Endeavor to reduce opportunities for conflict through prescriptive measures such as through information barriers to block or hinder the flow of information from one department / unit to another, etc.;
   h. The Company shall place appropriate restrictions on transactions in securities while handling a mandate of issuer or client in respect of such security so as to avoid any conflict;
   i. Not to deal in securities while in possession of material nonpublished information;
   j. Not to communicate the material non published information while dealing in securities on behalf of others;
   k. Not in any way contribute to manipulate the demand for or supply of securities in the market or to influence prices of securities;
   l. Not share information received from clients or pertaining to them, obtained as a result of their dealings, for their personal interest;

8. The Company's Compliance team shall have oversight on the business to ensure that internal controls are appropriate.

9. The Board of Directors of the Company and the Compliance team share the responsibility for keeping the Policy in place. Any situation or transaction involving an actual or potential conflict of interest should promptly be reported to the Compliance team and obtain their determination as to whether a conflict exists.

   Where a conflict arises and the Company is aware of it, it will disclose the conflict to the client prior to undertaking the business for that client or, if the Company does not believe that the disclosure is appropriate to manage the conflict, the Company may choose not to proceed with the transaction or matter giving rise to the conflict.

Measures to avoid or to deal or manage actual or potential Conflict of Interests.

Should a conflict of interest arise, it needs to be managed promptly and fairly. The Company puts in place following arrangements to ensure that:

i. There is a clear distinction between the different departments' operations;

ii. No single person will gather conflicting information, thus counterfeiting or hiding information from investors is minimized;

iii. The Company's employees are prohibited from investing in a financial instrument for which they have access to non-public or confidential information;

iv. Transactions by the Company's employees are neither performed nor executed by themselves.

v. Employees sign a contract of employment including confidentiality clauses. No associated person may disclose inside information to others, except disclosures made in accordance with the Company's policies and procedures, to other Company personnel or persons outside the Company who have a valid business reason for receiving such information;

vi. Each department will control the flow of information where, otherwise, the risk of conflict of interest may harm the interest of a Client;

vii. Relevant information is recorded promptly in a secure environment to enable identification and management of conflicts of interests;

viii. Adequate records are maintained of the services and activities of the

Company where a conflict of interest has been identified;

ix. In certain jurisdictions appropriate disclosure may be made to the Client in a clear, fair and not misleading manner to enable the Client to make an informed decision;

x. There is a periodic review of the adequacy of the Company's systems and controls.

xi. Employees are required to avoid conflicts of interest with activities they undertake outside company.

Violation and Consequences

Any non-adherence with the Policy will be subject strict action.

Disclosure

Periodic review of the Policy will be done at the Board Meeting of the Company. The same shall be on need basis. The Company reserves the right to make review and / or amend its Policy and whenever it deems appropriate.

In case you have any questions, please direct your query to our Compliance team **vei.helpme@gmail.com**

All concerned may take note of the above said policies and are advised to adhere to the same.

RISKMANAGEMENTPOLICY

RISK MANAGEMENT POLICY

Vijayranga Enterprises & Intermediaries (P) Limited, is a member of the Bombay Stock Exchange, and doing trades in the Equity segment, having its registered office at No.594/3, 8th Main Rd, MRCR Layout, Vijayanagar, Bengaluru-560040, Karnataka, India.

This document details the guidelines and procedures for Risk management Policy of VEI with main objectives on managing key risks in the broking business and lay down steps on how they are managed and mitigated, To define a clear and simple procedure for risk management relating to equity trades is to ensure consistency, uniformity, zero errors and transparency in various risk related activities. To assist in faster turnaround time thereby ensuring higher customer satisfaction and higher revenues.

RMS (Risk Management System): RMS helps the company to manage the trading risk and client from the volatility of the market.

1. DEFINITIONS:

Cash means – It is the clear balance available in the customer's ledger account in our books.

Securities Collateral Means- The amount of margin extended to the investor is calculated by reducing the haircut from the present market price of the share which is being pledged.

Exposure means - Exposure is the money in the trading account for trading in Intraday and Derivatives (F&O). Exposure is also known as Margin or Limit. If a client wants to trade for delivery, Intraday or in Derivative segments then he needs Exposure. Exposure varies from 1-5 times. For example, if VEI provides upto5 times Exposure. It means client can trade upto Rs. 50,000 with only Rs. 10,000 as Margin. Stock exchange sets the limit of minimum exposure 20% or peak margin requirements.

Exposure multiplier - The number of times that exposure is allowed on the underlying margin either on the availability of cash margin or on the availability of the stocks in our margin account/Pledged shares

2. RISK:

Head of Department and Risk Management Surveillance team should follow the prudent Risk Management policy devised by the Management for enrolling and activating the client and monitoring the trade done by him in Cash segment.

- Risk management policy is well documented and is made accessible to the clients whenever the same is demanded by the later.

- The Dealer/ Authorised Person carries out due diligence and risk profiling based on KYC procedures specified in KYC policy and Risk Management policy of the company. Types of Risk in Cash segment.
- Risk is generally used synonymously with the probability of known loss. Risk can be categorized into the following three types:

  - Low Risk
  - Technical Risk
  - High Risk

- To cover the above different types of risk, various types of margins are required is collected from the clients to allow to trade and also to minimize the risk arising to member when there is sudden down fall in the stock market.
- Margin is a minimum amount of funds and /or securities that must be held by a client in a trading account in order to allow trading in Cash market.
- As per SEBI circular we have to collect minimum of 20 % from the clients on upfront basis and others as per his trading practice and requirement of the Exchange.
- Types of margins with their terminology in cash market is given as under:

  i. Cash/Capital Markets:
     - VAR Margin
     - ELM Margin
     - M2M Margin
     - Additional Margin

3. MARGINS:

The client shall pay upfront applicable initial margins, mark to market losses, delivery margins, withholding margins, special margins or such other margins as applicable to the segment(s) in which the client trades. We permit them to trade with sole and absolute discretion to collect additional margins and the client shall be obliged to pay such margins within the stipulated time. The client understands that we shall liquidate/close out all or any of the client's positions for non-payment of margins or other amounts, outstanding debts, etc. and adjust the proceeds of such liquidation/close out, if any, against the client's liabilities/obligations. Any and all losses and financial charges on account of such liquidation/closing-out shall be charged to and borne by the client. In the event of death or insolvency of the client or his/its otherwise becoming incapable of receiving and paying for or delivering or transferring securities which the client has ordered to be bought or sold, we may closeout the transaction of the client and claim losses, if any, against the client. The client or his nominees, successors, heirs and assignee shall be entitled to any surplus which may result there from. Disseminating of the details regarding margin requirements and short fall in margin through an approved mode shall be considered as making a specific margin call to the client. We being an online broker disseminate this information online, on real time to all its clients in their individual account. Hence all clients are bound to log in to their trading account and keep themselves updated about their positions and margin requirements made available on real time basis at all points of time. The client has to maintain adequate margin for the positions taken in any segment at all time. However in case the margin available is lower than the margin required, the client's positions would be liquidated in a manner that the there is no shortfall of margin It shall solely be the client’s responsibility to ensure that adequate margins are available in the account.

Understanding of Limits: In the following ways limit shall be assigned in cash market segment. Limits shall be reset on daily basis by generating a file from the back office system at HO.

- **Cash Segment:**

  In cash market, VAR based trading pattern/system shall be applicable for all the clients.

Trading limit shall be provided to the client in cash segment based on Margin Pledge of stock after haircut and clear credit balance available in their ledger accounts.
Additional Limit provided to clients on case to case basis (Selling will be allowed for Early-pay in received for the Trade date).

- Clients are restricted in penny stock trade. However, if the clients are allowed to trade in penny stock like in Z group, ASM and GSM group, 100 % margin shall be charged or recovered from the client as per discretion of RMS team and systems are in place to ensure that these stocks are not counted for giving exposure to the client. Further, the management shall have the ultimate authority and can restrict the client for doing trade in particular securities including penny stocks.

- The scrips which are banned, illiquid &Z category for collaterals does not form part for calculating collateral margin. Management shall have the ultimate authority and can restrict client for doing trade in any particular securities/stocks including illiquid scrips or above mentioned categories.

- Trade is regular monitored of clients account who has been given collateral in the form of single or multiple stock
- The company shall decide the component of cash and non-cash collaterals from time to time either in general or for any particular client as the case may be.
- For valuation of collaterals, the market rate shall be considered as closing price of T-1 day. Haircut shall be VAR rate and subject to minimum of 20% or at percentage which may be decided from time to time. It can be applied based on categorization of scrips in few categories.
- We ensure that the collaterals received are from the client's designated DP account and not from third party as it is system driven there is no scope of third party collaterals.
- Branch Manager/Dealers ensures that orders are placed through CTCL/BOLT/NEAT Terminals with in the exposure limits applicable to clients as decided by the RMS Team and the HO.
- In case of cash market for trading in equity segment ensure that 35 % coverage is maintained all the time by the client and such calculation is done on daily basis by the RMS team and is informed to the client accordingly.
- In case of derivatives segment, one time exposure is allowed and initial margin is mandatory to trade in Derivatives and Commodity segment.

- In Derivatives and Commodity segment position shall not be allowed to carry forward with Short margin.
- Un-cleared cheque will not be considered as Margin, system shall consider Additional Margin for Funds received for Margin only on Clearance of the cheque.
- AP's to collect MTM margin immediately on T day in case the margin has fallen below the required level as per the policy decided by HO, in other case on next day (i.e. T+1 day).
- In setting exposure limits to the client ,the factors that will be considered like client's risk profile, risk appetite, loss bearing capacity, payment history, market volatility, risk management policy of the company and such other factors or conditions which the company may consider relevant for the purpose from time to time.
- Enhancing/Adjusting the Exposure or available Margin for Clients during the day:
- During the trading hours ,exposure or available margin can be enhanced /adjusted for clients based on the following :¬ On receipt of funds through RTGS/NEFT/Transfer Cheques/Bank Recco Cheques (with prior approval) ¬ On withdrawal of funds (with prior approval of RMS Team) ¬ On receipt of collateral by client to Margin Pledge demat account.
- On withdrawal of collateral from client's collateral Demat account (with prior approval of RMS Team)
- Exposure may be adjusted on receipt of news from market (market wise, client wide or security wide, if any), general volatility in the market etc.
- In case of funds received through RTGS, funds should have been received and the necessary entries in the back office are passed.
- In case of receipts of collateral, provide details of collateral transferred in client's beneficiary collateral Demat account from the concerned client.
- The exposure shall be enhanced only after adjusting the shortfall, if any from the additional margin received during the day.
- Positions of the client may be closed out to the extent of margin shortfall on the T+1 basis /Real time monitoring basis.
- If there is a Mark to Mark loss VEI has rights to square off the positions as per RMS policy
- While computing margin shortfall, value of unapproved securities shall not be considered.
- While selling the securities/ closing the client positions, we may not take into consideration Cheques showing unclear although deposited by the client with us until clear proceeds of such instruments are received by us in its bank account. For this purposes Demand Draft / Pay order will not be taken into consideration.
- We shall have the right to sell client securities in case of Ageing of debit and margin shortfall in the client account.
- Conditions under which a client may not be allowed to take further position or we may close the existing position of a client in all markets
    - Client is not having adequate margins as per conditions in Risk Management policy.

- The client has not been able to meet his pay-in obligations in cash by the schedule date of pay-in irrespective of the value of collaterals available with us
- Clear proceeds of the cheque deposited by the client to meet the pay-in obligations have not yet been received by us.
- The client has not made payment for Market to Market loss
- In Ledger Intra-day positions we shall have right to close out any intra-day positions taken by the client after a defined 'Cut-off' time (Presently 15 minutes before close of market).
- Client is trading in "illiquid" scrips and volume in his account exceed internal cut off limit fixed by us as per RMS Illiquid policy.

Penalty levied to Clients for Short collection of Margin/Other Margin/MTM Margin as specified by Exchange, will be imposed/collect penalties from Clients as per Exchange in Derivatives and Commodity segment. Further we reserve the right to keep client on a square off mode or can reduce position in case where client has penalty imposed by Exchange in case 3 times or more during a month for Short margin/MTM.

CUSPA (Client Unpaid Securities Pledgee Account)

This means Client Unpaid Securities Pledge Account. As per SEBI circular SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2022/153 dated 11th Nov 2022, new rule has come in force for the unpaid securities.

The new rule is summarized below.
Regarding the unpaid securities (i.e., the securities that have not been paid for in full by the clients on T Day), such securities shall be transferred to respective client's Demat account followed by creation of an auto-pledge (i.e., without any specific instruction from the client) with the reason "unpaid", in favour of a separate account titled –client unpaid securities pledgee account (CUSPA) on Pay Out day.

Setting up Client Exposure Limit: The limit shall be provided as per the availability of the margin. In case of cheque, the limit shall only be given upon clearance only. No limit will be given on the CUSPA stock.

Kindly refer to SEBI circular no. CIR/HO/MIRSD/DOP/CIR/P/2019/75 dated 20.06.20219 - Accordingly, below mentioned is the process we follow for the Pay Out +5 days debit codes:

Shares bought and not paid on T Day, and then the shares go to CUSPA as per the SEBI guidelines. In case the client does not pay for the shares bought on T Day, then on Pay Out +5 days day we liquidate those shares pledged marked in CUSPA.

Further exposure client will not be allowed as the debit continues (T+2+5) as per SEBI circular dated 26.09.2016 in all segments.

RMS Team generates on daily basis, debtors/client's list with secured and unsecured/uncovered amount along with the ageing list.

Absolute debit balance in client account in excess of RS.5 LAC Sand/or in excess of 7 days shall be separately monitored by RMS Team.

The following are some of the indicative actions which may be initiated by RMS Team in a Volatile Market Conditions:

- Increase the haircut on Collaterals
- Increase the Margin rate
- Reduce intraday exposure /Multipliers
- Disallow scrip to trade
- Liquidation of positions
- Disallow client to take exposure (based on news)
- Provide Margin calls to clients after valuing their portfolio

Failure of the seller to deliver securities shall result in buy-in-auction for the shares by Clearing Corporation as per auction schedule declared periodically. Currently auction shall be conducted on Expiry+3 days and settled on Expiry+4 days. The auction amount shall be charged in case of short delivery of shares. Failure to procure shares in auction shall be closed out.

Please note that RMS will square off open position in Stock Futures/Option's which has been mandated by Exchanges for physical settlement, at least 4 days before expiry day. You can choose to rollover your positions or close the same before 4 days including expiry day E.g. July expiry contracts needs to be closed/rollover by you on or before 4 days including expiry day or else the same would be closed by RMS any time of last 4 days expiry. Also all open position in such contract's will be on-square off mode on last day of expiry on Thursday, Hence for every expiry VEI RMS will square off open positions in Stock Futures / Options on the last Thursday of every expiry.

To take adequate care while trading in options as in case of illiquid contract it will be difficult to square-off position which may result in physical settlement. In case RMS is unable to square off, then such contracts will be physically settled and client will be required to honour the securities and funds settlement obligations resulting out of such settlement.

Short Selling

1. "Short selling" shall be defined as selling a stock which the seller does not own at the time of trade.
2. All classes of investors, viz., retail and institutional investors, shall be permitted to short sell.
3. Naked short selling shall not be permitted in the Indian securities market and accordingly, all investors would be required to mandatorily honor their obligation of delivering the securities at the time of settlement.
4. No institutional investor shall be allowed to do day trading i.e., square-off their transactions intra-day. In other words, all transactions would be grossed for institutional investors at the custodians' level and the institutions would be required to fulfill their obligations on a gross basis. The custodians, however, would continue to settle their deliveries on a net basis with the stock exchanges.
5. Vijayranga Enterprises & Intermediaries (P) Limited shall be mandated to collect the details on scrip-wise short sell positions, collate the data and upload it to the stock exchanges before the commencement of trading on the following trading day..

Exceptional Circumstances:
All exceptional circumstances are escalated to the management for immediate resolution. This policy has been adopted by the trading member as on 3rd November 2022 and may be revised from Time to Time

GENERAL RISK COVERAGE: - The Company have adequate insurance cover for different types of exposures, including but not limited to fidelity insurance, To reduce the systemic risk, Stock Broker Indemnity Policy of Rs. 5 Lacs + Rs.5 lacs through the membership with ANMI and BBF which covers losses on account of trading as well as back office losses shall be obtained. The company's risk policies and measurements and

reporting methodologies are subject to regular review on annual basis or when there are significant changes to the products, segments.

As company is mainly into franchisee (AP) model, the franchisee is responsible for any client dues. This gives additional safety to the company from client default.

SURVEILLIANCE POLICY (STOCKBROKERS)

SURVELLIANCE POLICY

Surveillance is the process of collecting and analyzing information concerning markets in order to detect unfair transactions that may violate securities related laws, rules and regulations. In order to ensure investor protection and to safeguard the integrity of the markets, it is imperative to have in place an effective market surveillance mechanism. The main objective of the surveillance function is to help maintain a fair and effective market for securities. Therefore, we have decided to undertake adequate measures for ensuring effectiveness and efficiency of the trading and depository system. The Company with the above motive in mind has framed Surveillance policy focusing on:

i. To establish a surveillance mechanisms and controls in the operations/trading activity
ii. To put in place appropriate ontrols for the detection and reporting of suspicious trading activities in accordance with applicable laws/laid down procedures.
iii. To comply with applicable laws and regulatory guidelines.

The Stock Exchange(s) are providing alerts based on predefined criteria to the all the stock brokers through their portals. As per applicable Circulars, the Company is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with provisions of PMLA (Maintenance of records) Rules,2005.

TYPE of TRANSACTIONAL ALERTS DOWNLOADED BY THE EXCHANGE

Sr. No	Transactional Alerts	Segment
1	Significantly increase in Client Activity	Cash
2	Sudden Trading activity in dormant account	Cash
3	Clients/Group of client(s), deal in common scrip's	Cash
4	Client(s)/Group of Client(s) is Concentrated in a few illiquid scrip's	Cash
5	Client(s)/Group of Client(s) dealing in Scrip in minimum lot size	Cash
6	Client/Group of Client(s) Concentration in A scrip	Cash
7	Circular Trading	Cash
8	Pump and Dump	Cash
9	Reversal of Trades	Cash & Derivatives
10	Order Book Spoofing i.e. large orders Away from market	Cash

Additional Monitoring Criteria:

In addition to above, the company has also implemented the mechanism to generate alerts as per

provided in exchange circulars based on following criteria:-

a. Trading activity in a single day by one client or group of clients who have contributed more than 25% in single scrip.

b. A client or a group of clients who are either new client/ clients or who have reactivated their trading account after significant time gap and who have contributed more than 50% of the total trading volume of a single scrip.

c. Client or a group of clients dealing frequently in small quantities in a scrip.

d. Trading activity of a client found to be disproportionate considering a reported income range details or net worth.

e. A client who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details etc. at least twice in a month.

f. A client or a group of clients who have been found to have direct or indirect connection with a listed company and who have executed any transactions prior to any dissemination of any price sensitive information by such listed company.

g. client who has received shares of a listed company through multiple off- market transfer and has pledged such shares.

h. Not allowing trades of entities which are banned by SEBI/Exchange and other regulators.

i. Clients who have debit balance in their ledgers continuously for a certain period of time or who defaults in making payment/delivery. This will be monitored by RMS team and does follow up with clients/APs and if required will be restricted from further trading.

PROCESSING AND REVIEW AND DISPOSAL OF ALERTS:-

The surveillance process shall be conducted under overall supervision of its Compliance Officer and he / she shall be the designated official tasked with the review, processing and disposal of alerts.

If the designated official finds after review and due diligence that the alert is required to be closed, the official shall close the same with appropriate remarks.

If the designated official after due diligence and making such inquiry, as such official finds necessary, comes to a conclusion that the given alert warrants an action, the official will forward the same with his/her views to the Designated Director for his/her approval.

In order to review, analyze and dispose off the alerts, the designated official may:-

a. Seek explanation / information from such identified Client(s)/ Group of Client(s)for entering into such transactions. Letter/email to be sent to client asking the client to confirm that client

has adhered to trading regulations and details may be sought pertaining to source of funds and securities, economic sense and trading pattern.

b. Seek documentary evidence such as Bank Statement/Demat Transaction Statement, Financial Statements or any other documents to support the trading pattern of the client.

After analyzing the documentary evidences, including the Bank / Demat statement, the observations shall be recorded for such identified transactions or Client(s) / Group of Client(s).

If the designated official finds that action in respect of such alert is warranted, he/she shall take such actions including filing STR with FIU-India, informing to Stock Exchanges and Depository and/or discontinue the relationship with the client.

In case of adverse observations, there port of such instances along with adverse observations and details of actions taken shall be submitted to the Stock Exchanges/ Depository within 7 days from date of identification of such instances.

In case the client does not cooperate or does not revert within reasonable period, Exchange to be informed based on the information available with the member.

All efforts shall be made to dispose off a given alert within 45days of its receipt/ generation.

The records of alerts generated, disposed of as closed and details of action taken wherever applicable shall be maintained with such security measures as would make such records temper proof and the access is available on to designated officials under the supervision of the Compliance Officer.

MONITORING AND RECORD MAINTENANCE

The surveillance process shall be conducted under overall supervision of its Compliance Officer and based on facts and circumstances, he / she is required to take adequate precaution.

A quarterly MIS shall be put up by the Compliance Officer to the board and the Designated Director giving number of alerts generated during the quarter, number of alerts closed, number of alerts on which action taken with details of action taken and number of alerts pending at the end of the quarter along with reasons for pendency and action plan for closure. The Board as well as the Designated Director shall be apprised of any exception noticed during the disposal of the alerts.

Internal auditor shall review this policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

REPORTING OF ALERTS

The Company shall provide duly approved status of the Alerts on a Quarterly basis to the exchange in the format prescribed by the exchange within 15 days from the end of the quarter.

In case zero alert during the quarter, NIL report need to be submit to the exchange as per the prescribed format.

REVIEW:

This policy will be reviewed by the Designated Director, as and when there are any changes introduced by any statutory authority or at least once in a year to ensure that same is updated and in line with market trends, updated regulations and practices.

SURVEILLANCE POLICY (DEPOSITORY PARTICIPANT)

SURVIELLANCE POLICY for Depository Participant (DP):

SURVEILLANCE POLICY: The objective of this policy is to have in place an effective surveillance mechanism to ensure investor protection and to safeguard the integrity of the Depository Participant. The surveillance to spot adverse situations and to pursue appropriate preventive actions. The DP business is closely linked to investor protection and, in particular, to the prevention of improper practices. This monitoring is required to analyses the pattern of the clients Transactions and other activities in order to observe whether any transaction done intentionally, which is against the fundamental objective of the DP and Regulators. Thus, as a DP, we are the first level to ensure that our Client(s) are not misusing the Depository system by indulging in manipulation or any other illegal activities which can cause risk to the integrity of the DP.

Objectives of framing a DP surveillance policy covering

- Generation of suitable surveillance alerts which may be guided by indicative themes
- Review and disposal of transactional alerts provided by NSDL/ CDSL
- Disposal of alerts within 30days from the date of alerts generated at Participant send and alerts provided by NSDL/CDSL.
- ReportingtoNSDL/CDSL/FIUandotherauthoritiesasapplicableincaseofany abnormal activity.
- Documentation of reasons for delay, if any, in disposal of alerts.
- Framework of appropriate actions that can be taken by the Company as per obligations under Prevention of Money Laundering Act (PMLA).
- Record maintenance for the period as stipulated under applicable statutes.
- The surveillance policy shall be reviewed once in a year.

Indicative themes:

- Alert for multiple Demat accounts opened with same demographic details:
- Alert for accounts opened with same PAN/mobile number/email id/bank account no./ address considering the existing Demat accounts held with the Participant.
- Alert for communication (emails/letter) sent on registered Email id/address of clients are getting bounced.
- Frequent changes in details of Demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.

- Frequent Off-Market transfers by a client in a specified period
- Off-market transfers not commensurate with the income/Net-worth of the client.
- Pledge transactions not commensurate with the income/Net-worth of the client.
- Off-market transfers (High Value) immediately after modification of details in Demat account
- Review of reasons of off-market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales
- Alert for newly opened accounts where in sudden Increase in transactions activities in short span of time and suddenly holding in Demat account becomes zero or account becomes dormant after some time.
- Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.

1. Obligation of Depository Participants regarding Client due diligence:

The following activities required to be carried out by Participant for client due diligence is being reiterated:

a. Participants are required to carry out the Due Diligence of their client(s) on an on-going basis.

b. Participants shall ensure that key KYC parameters of the clients are updated on a periodic basis as prescribed by SEBI and latest information of the client is updated in Depository System.

2. Obligation of Depository Participants to w.r.t. Processing of Alerts:

a. Participants are required to maintain register (electronic/physical) for recording of all alerts generated.

b. While reviewing alerts, Participant shall obtain transaction rationale, verify Demat account statement and also obtain supporting documents as required from the client.

c. After verifying the documentary evidences, Participants shall record its observations for such identified transactions of its Client.

d. With respect to the transactional alerts to be provided by Depository, Participants shall ensure

that all alerts are reviewed and status thereof (Verified & Closed/Verified & Reported to

Depository) including action taken is updated within 30 days, on the NSDL e-PASS portal / CDSL portal. The procedure w.r.t sharing of alert by NSDL/CDSL with Participants and report submission by Participants in this regard will be provided separately.

e. With respect to the alerts generated at the Participants end, Participants shall report instances with adverse observation, along with details of action taken, to NSDL/CDSLwithin7daysof the date of identification of adverse observation. Detailed procedure w.r.t reporting of alert by Participants will be provided separately.

3. Obligation of Compliance officer and Internal Auditor / Concurrent Auditor of the Participants:

a. The surveillance activities of Participant shall be conducted under overall supervision of its Compliance Officer.

b. A quarterly MIS shall be put up to the Board on the number of alerts pending at the beginning of the quarter, generated during the quarter, processed and acted upon during the quarter and cases pending at the end of the quarter along with reasons for pendency and action plan for closure. Also, the Board shall be apprised of any exception noticed during the disposal of alerts.

c. Internal auditor of Participant shall review the surveillance policy, its implementation, effectiveness and review the alerts generated during the period of audit. Internal auditor shall record the observations with respect to the same in their report.

d. Internal Auditor shall verify that the quarterly MIS is prepared and placed before the Board of the Participant.

4. Obligation of Quarterly reporting of status of the alerts generated by Participants:

Participants are also required to provide duly approved status of the alerts on a quarterly basis, in the following format to NSDL within 15 days from end of the quarter.

a. Status of Alerts generated by the Depository:

Name of Alert	No. of alerts pending at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts Verified & closed in the quarter	No. of alerts reported to Depository	No. of alerts pending for process at the End of quarter

b. Details of any major surveillance action taken (other than alerts reported to Depository), if any, during the quarter:

Sr. No.	Brief action taken during the quarter

c. Participant who do not have anything to report, need to submit 'NIL Report' within 15 days from end of the quarter.

d. The above details shall be uploaded by the Participants on NSDL e-PASS Portal/CDSL portal.

e. The afore mentioned quarterly system of reporting shall be effective from the quarter ending December 2021.

5. Penalty in case of late /non-submission of Quarterly Reporting of status:

In case of late/non-submission of quarterly report of the alerts generated by Participant as mentioned at Point no.2 above, Participant shall be liable for penalty.

6. Disciplinary action for non-fulfillment of Surveillance obligation by Participant:

a. Participant may note that during inspection, if it is observed that the Participant has not fulfilled their surveillance obligations, then appropriate disciplinary action shall be initiated against the concerned Participant.

b. Any non-compliance with respect to surveillance obligations which may inter alia include delay in processing of alerts generated by Participant/ provided by NSDL/CDSL and repeated instances of delay in reporting of the status of alerts, may result in further disciplinary action as deemed fit in terms of Business Rules and Bye-laws of Depositories.

c. It may further be noted that aforesaid measure does not preclude SEBI/ Depository to take any further action(s), if the facts and circumstances so demand.

ELECTRONIC FUND POLICY

POLICY WITH REGARD TOP RE-FUNDED INSTRUMENTS/ ELECTRONIC FUND TRANSFER

The following policy has been adopted by Vijayranga Enterprises & Intermediaries (P) Limited with regard to Pre-funded Instruments/Electronic Fund Transfer.

1. Pre-funded instruments such as Pay Orders/Demand Draft/Bankers' Cheque etc more than Rs.50,000/- (Rupees Fifty Thousand Only) are not to be accepted unless accompanied by the following details duly certified by the Issuing Bank:-
   a. The name of the account holder and where from it is debited
   b. The number of bank account from where it is debited

2. The mode of certifications shall be as prescribed in SEBI Circular no. ClR/MlRSD/03/2011dated July 9, 2011

3. Regarding the electronic fund transfer, we should also verify the account number and account holder's name where from the transfer has come.

4. There should be verifications that money has come from the accounts of respective clients only.

5. If payment is not received from the said designated bank account than such fund will be marked and transferred as suspense and after receiving necessary documents from client it will be credited to his/her account.

6. The audit trail shall be maintained for the same.

IT POLICY

About Vijayranga Enterprises & Intermediaries (P) Ltd

SEBI Registration No: INZ000319033
BSE Member ID: 6291
NSDL: IN304957
CIN: U66120KA2010PTC053979

Table of contents

Part A

23. Operations Management
24. Incident Management Procedures
25. Segregation of Duties
26. Separation of Test and Operational Facilities
27. System Planning and Acceptance Protection Against Code
28. Information Back-up
29. System Security Checking
30. Disposal of Media
31. Data Access Control
32. User Registration and Management
33. User Password Management
34. Segregation of Networks
35. Operating System Access Control
36. Systems Development and Maintenance
37. Input Data Validation
38. Control of Internal Processing
39. Cryptographic Controls
40. Safeguarding of Vijayranga Enterprises & Intermediaries (P) Ltd Records

1. Purpose

Information Technology (IT) is the most important enabler of Business. The information technology provides new advantages to business operations and can be used as a tool for business process transformation that crosses several functional lines.

Cyber space is a complex environment consisting of interactions between people, software And services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

In the light of the growth of IT in our organization, providing right kind of focus for creating Secure computing environment and adequate trust&confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities.

The protection of information infrastructure and preservation of the confidentiality, integrity
and availability of information in cyberspace is crucial. The policy aims to protect information and information infrastructure from cyber incidents through a combination of processes, guidelines, technology and cooperation.

All the Policies are laid down according to the guidelines issued by

I. Ministry of Electronics & Information Technology, Government of India.
II. Securities and Exchange Board of India
III. National Stock Exchange of India Ltd.
IV. Bombay Stock Exchange Ltd.
V. ISO27001, COBIT5

2. Objectives

The objective of this policy is to ensure proper access to and usage of IT resources and prevent their misuse by the users. Use of resources provided by Vijayranga Enterprises & Intermediaries (P) Ltd imply the user's agreement to be governed by this policy, manage the risk of security exposure or compromise of Vijayranga Enterprises & Intermediaries (P) Ltd information assets; Designate responsibilities for the protection of Vijayranga Enterprises & Intermediaries (P) Ltd sensitive information and optimize the integrity and reliability of information assets;

3. Scope

This policy is applicable to entities, staff and all others who have access to or manage Vijayranga Enterprises & Intermediaries (P)Ltd information. This policy encompasses all information systems for which Vijayranga Enterprises & Intermediaries (P) Ltd has administrative responsibility. It addresses all digital information which is created or used in support of Vijayranga Enterprises & Intermediaries (P) Ltd business activities.

Information security refers to the protection of information from accidental or unauthorized access, destruction, modification or disclosure. Digital information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means.

Digital information is relayed in a variety of methods, including desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith. This policy must be communicated by the systems department to all employees and all others who have access to or manage Vijayranga Enterprises & Intermediaries (P) Ltd digital information.

4. Preface

This policy is a statement of the goals, ethics, responsibilities and accepted behaviors

required to establish and maintain Vijayranga Enterprises & Intermediaries (P)Ltd information security objectives; it sets the direction, offers broad guidance and defines management's requirements for digital information security related processes and actions. Compliance is mandatory.

This policy follows the framework of ISO27001 for Security Policy guidelines and is consistent with existing Vijayranga Enterprises & Intermediaries (P)Ltd policies, rules and standards. This policy documents many of the security practices already in place.

5. Governance

Technology committee is responsible for creation of information security policy and agrees that every person employed by or on behalf of Vijayranga Enterprises & Intermediaries (P) Ltd has important responsibilities to continuously maintain the security and privacy of Vijayranga Enterprises & Intermediaries (P) Ltd data.

Technology committee of Vijayranga Enterprises & Intermediaries (P)Ltd comprises of following members

For Financial Year2026-27

Sl. No	Name	Designation	Position in Committee
1	Mr. S N Ravi	Director	Chairman
2	Mrs. Tejaswini Srivijay Sastry	CEO	Member
3	Ms. Sahana K	Executive	Member

6. Document Change Management.

Requests for changes to this policy should be presented by the Vijayranga Enterprises & Intermediaries (P) Ltd information Security team to the Technology Committee. If the committee agrees to the change(s), the Information system department will be responsible for communicating the approved change(s) to the Vijayranga Enterprises & Intermediaries (P) Ltd employees. This document is maintained by the office of Systems Department for the organization, supporting policies and standards will be reviewed on an annual basis by the technology committee.

7. Information Security Policy

Information is among Vijayranga Enterprises & Intermediaries (P)Ltd is most valuable assets and Vijayranga Enterprises & Intermediaries (P) Ltd relies upon that information to support its mission of supporting trading through its applications, research and support as well as its business activities. Information must be protected from the time it is created, through its useful life, and authorized disposal since quality and availability of that information is key to Vijayranga Enterprises & Intermediaries (P)Ltd‟s ability to carry

out these missions.

Therefore, the security of Vijayranga Enterprises & Intermediaries (P)Ltd‟s information, and of the technologies and

systems that support it, is the responsibility of everyone concerned. Each authorized user of Vijayranga Enterprises & Intermediaries (P) Ltd information has an obligation to preserve and protect said information assets in a consistent and reliable manner. Information must be classified and protected based on its importance to business activities, risks and security practices as defined in ISO 27001, a code of practice for Information security management, and as implemented by this policy.

Security controls provide the necessary physical, logical and procedural safe guards to accomplish those goals. Information security management enables information to be shared while protecting the information and its associated computer assets including the network over which the information travels. Vijayranga Enterprises & Intermediaries (P)Ltd systems department are responsible for ensuring that appropriate physical, logical and procedural controls are in place on these assets to preserve the confidentiality, integrity, availability and privacy of Vijayranga Enterprises & Intermediaries (P) Ltd information.

Privacy and Handling of Private Information

- Privacy of an individual's information must be respected throughout its life time.
- Vijayranga Enterprises & Intermediaries (P) Ltd's systems hold personal identifiable information (i.e., any information that is unique to any individual) to carry out the business of Vijayranga Enterprises & Intermediaries (P) Ltd.
- The protection of the privacy of personal information is of utmost importance and Vijayranga Enterprises & Intermediaries (P) Ltd must conduct business so as to protect the rights of privacy of all members of the public, business partners, and Vijayranga Enterprises & Intermediaries (P) Ltd community.
- All Vijayranga Enterprises & Intermediaries (P)Ltd employees with access to personal information
  Are required to respect the confidentiality of that personal information.
- Personal data, including information about clients, employees, members of the public, organizations and business partners, collected and maintained by Vijayranga Enterprises & Intermediaries (P) Ltd must:
    - Be used only for the stated purpose for which it was gathered;
    - Be gathered in lawful and fair circumstance;
    - Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;
    - Not bed is closed without specific consent or as authorized by law;
    - Be available for review by authorized individuals;
    - Be corrected if errors are known to exist or if the individual identifies errors
    - Be erased where appropriate if the individual requests consistent with applicable laws; and
    - Be protected using system access controls, or be stored in a locked cabinet or office. (If this information is stored by a third-

party, the third-party must contractually abide by these rules.)

- Be destroyed in a manner consistent with that required by law or

regulations.

8. Individual Accountability

Individual accountability is the cornerstone of any security program. With out it, there can be no security. Individual accountability is required when accessing all Vijayranga Enterprises & Intermediaries (P) Ltd electronic resources or when terminating employment. Access to Vijayranga Enterprises & Intermediaries (P)Ltd computer systems and networks is provided through the use of individually assigned unique computer identifiers known as user-ID and password. Individuals who use Vijayranga Enterprises & Intermediaries (P) Ltd computer resources must only access resources to which they are authorized.

Passwords must be treated as confidential information and must not be disclosed. All individuals are responsible for all activities performed under their user-ID. For the user's protection and for the protection of Vijayranga Enterprises & Intermediaries (P) Ltd resources, passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared. Upon termination of employment, individuals are required to archive or delete information according to record retention policy.

9. Confidentiality/Integrity/Availability

All Vijayranga Enterprises & Intermediaries (P) Ltd information will be protected from unauthorized access to help maintain information's confidentiality and integrity. The information owner will classify and secure information within the irjurisdiction based on the data classification guidelines according to the information's value, sensitivity to disclosure, consequences of loss or compromise and ease of recovery.

Information will be readily available for authorized use as needed by the user in the normal performance of their duties. Appropriate processes will be implemented to ensure the reasonable and timely recovery of all Vijayranga Enterprises & Intermediaries (P) Ltd information, applications and systems, regardless of computing platform, should that information should not become corrupted, destroyed, or unavailable for a defined period.

10. Business Impact Analysis

Business impact analysis will be performed periodically to determine the criticality of Vijayranga Enterprises & Intermediaries (P) Ltd processes and establish a schedule for backup and recovery of those systems and data to ensure their timely recovery in the event of an extended outage. When performing a business impact analysis, the systems department as charged by management, will Identify all key business processes and assess their criticality to the operation of Vijayranga Enterprises & Intermediaries (P) Ltd.
The systems department will determine maximum acceptable time to recover each key business process in the event of a disruption; For each critical process, an inventory will

be developed of all of the assets required to perform the process or to resume the process

in the event of a disaster. Considerations of assets will include but are not limited to staff, accommodations, communications, IT assets, networking and data;

- Perform a threat analysis to determine the threats the organization and its data are subject to. These threats could include natural disasters or man-made events;

- Perform a risk assessment to determine the likelihood that a threat would or could occur; Develop and test plans to recover the assets within the time frame required to meet the requirements of the lines of business.

11. Security Organization Policy

Vijayranga Enterprises & Intermediaries (P) Ltd's Information System Department is responsible for researching and managing information security issues. The Team reports to the chairman of the technology committee who is responsible for its organization and leadership..

The duties of the systems department is to:

- Maintain and update the threat landscape for the organization on a regular basis including staying up to date about the latest security threat environment and related technology developments.

- Establishing a cyber security program and business continuity programme and for drafting of various security policies e.g., Information security policy, Data governance and classification policy, Access control policy, Acceptable use of assets

- Ensuring review of the Information Security Policy by internal and/or external subject matter experts to check for the adequacy and effectiveness of the ISMS programme

- Reviewing and updating the cyber security policy documents.

- Defining rules for secure and acceptable use of communication channels for the business requirements of the department/organization.

- Developing and implementing a security architecture for the organization by leveraging technology and understanding of the threat landscape.
- Establishing and reviewing the Risk Assessment methodology and selection of appropriate controls for risk mitigation by leveraging technology and an understanding of the threat landscape in the organization.

- Interacting with regulatory bodies and external agencies that could be of help to

Maintain information security for the organization, e.g. CERT-In, NSE.

- Ensuring that the following activities are carried out at regular intervals, either directly or through the deployment of subject matter - Log review, analysis and exception reporting

- Develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of Vijayranga Enterprises & Intermediaries (P) Ltd;

- Provide information security consulting to Vijayranga Enterprises & Intermediaries (P)Ltd regarding security threats that could affect Vijayranga Enterprises & Intermediaries (P) Ltd computing and business operations and make recommendations to mitigate the risks associated with these threats;

- Assist management in the implementation of security measures that meet the business and academic needs of Vijayranga Enterprises & Intermediaries (P) Ltd;

- Develop and implement security training and awareness programs that educate Vijayranga Enterprises & Intermediaries (P) Ltd employees, contractors and vendors with regard to Vijayranga Enterprises & Intermediaries (P)Ltd's information security requirements;

- Investigate and report to the management regarding breaches of security controls, and implement additional compensatory measures when necessary to help ensure security safeguards are maintained;

- Assist with the development, implementation and maintenance of disaster recovery processes and techniques to maintain Vijayranga Enterprises & Intermediaries (P) Ltd business continuity in the event of a disaster or extended period of computer resource unavailability.

12. User Training

An information security awareness program will be developed, implemented, and maintained to address security education for Vijayranga Enterprises & Intermediaries (P) Ltd employees. The awareness program will review information security policy, threats and concerns, and the proper use of information processing facilities (e.g. logon procedures and use of software packages) to minimize possible security risks.

The program will additionally include the procedure to follow to report incidents (security breach, threat, weakness or malfunction) that might have an impact on the security of

Vijayranga Enterprises & Intermediaries (P) Ltd information.

Reporting Security Weaknesses

- Users of Vijayranga Enterprises & Intermediaries (P) Ltd Information technology resources will be required to note and report any observed or suspected security weaknesses or threats to the appropriate manager of Internal Control via **veiblr@gmail.com**

- They must report these weaknesses as soon as possible. Users must not attempt under any circumstances to prove a suspected weakness. This is for their own protection, as testing weaknesses could be perceived as a potential misuse of the system.

- Information Technologies established specifically to research Information assurance as a legitimate academic pursuit are not restricted by this reporting policy.

Procedures must be established for reporting security software malfunctions. The following should be considered:

- The symptoms of the problem and any messages appearing on the screen should be noted;
- The computer must be isolated, if possible, and use of it stopped until the problem has been resolved;

The matter should be reported immediately to the systems department team, for appropriate investigation.

13. Physical and Environmental Security

Critical or sensitive Vijayranga Enterprises & Intermediaries (P) Ltd business information processing facilities must be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls to protect from unauthorized access, damage and interference.
Physical security perimeters should be established in Vijayranga Enterprises & Intermediaries (P) Ltd environments where servers are stored or operational in wiring closets for network and telephonic connections, where printers used for printing confidential or sensitive information, and any other location.

All devices on the network of Vijayranga Enterprises & Intermediaries (P) Ltd should not be accessible without proper Authentication (Preferably Biometric Authentication for Physical access to Computer / Data Center at Office Premises).

The systems department team will perform periodic threat and risk analysis to determine

the extent of the perimeter vulnerabilities.

14. Clean Desk and Clear Screen

Sensitive information must be removed from view and physically secured when not in use. Measures must be taken to ensure that such information cannot be read or copied by unauthorized persons.

Physical security for the machine when unattended is one approach. The use of computer screen savers or similar technology is required to ensure that sensitive information is not displayed after a specified period of inactivity. When unattended or physically unsecured for more than a few minutes, all computers must be screen locked with password protection.

15. Communications and Network Management

Vijayranga Enterprises & Intermediaries (P)Ltd network monitoring follows best practice to the extent appropriate resources are available for staffing and monitoring tools.
Third party connections to any portion of the Vijayranga Enterprises & Intermediaries (P) Ltd network could compromise the integrity and confidentiality of data on the Vijayranga Enterprises & Intermediaries (P)Ltd network. Third party network connections are only allowed with prior approval by the systems department to ensure that security measures are in place to maintain the current level of security on Vijayranga Enterprises & Intermediaries (P) Ltd networks.

16. Network Management

Vijayranga Enterprises & Intermediaries (P) Ltd implements a range of network controls to maintain security in its trusted, internal network, and to protect connected services and networks. The network includes any device that is attached via a wired or wireless connection with an IP (Internet Protocol) address.

Host Scanning.

Systems department reserves the right to scan any device attached to the Vijayranga Enterprises & Intermediaries (P) Ltd network on a periodic and tiered basis to ensure optimal configuration to protect against known vulnerabilities and to advise management of unencrypted storage of highly sensitive/confidential data.

I. Access to Internet and Intranet

- A user should register the client system and obtain one time approval /permission

From the system department before connecting to the Vijayranga Enterprises & Intermediaries (P)Ltd network.

- Users should not undertake any activity through any website or applications to bypass filtering/Policy/Firewall/UTM of the network or er for many other

Unlawful acts which may affect the network's performance or security.

- Users are not allowed to change the NIC configuration, IP address or any other parameters set for accessing the company's LAN&WAN without permission.

- Users shall not connect any other devices to access Internet/any other network in the same client system configured for connecting to LAN/WAN of the company without permission.

- It is the responsibility of the user to ensure that the client system is free from any Virus/Malware/Potential threat softwares /pirated copy of softwares before connecting to the company's network.

II. Access to Vijayranga Enterprises & Intermediaries (P)Ltd Wireless Networks

For connecting to a Vijayranga Enterprises & Intermediaries (P)Ltd wireless network, user should ensure the following:

- A user should register the access device and obtain one time approval / permissionfromthesystemsdepartmentbeforeconnectingtheaccessdeviceto the Vijayranga Enterprises & Intermediaries (P) Ltd wireless network.

- Wirelessclientsystemsandwirelessdevicesshouldnotbeallowedtoconnectto the Vijayranga Enterprises & Intermediaries (P) Ltd wireless access points without due Authentication.

- To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

- It is the responsibility of the user to ensure that the device is free from any Virus/Malware/Potential threat softwares/pirated copy of softwares before connecting to the company's Wi-Fi network.

III. Filtering and blocking of sites:

The systems department may block content over the Internet which is in contravention of the relevant provisions of the Government Laws and other applicable laws or which may pose a security threat to the network.

The systems department may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the network security and productivity of the users/organization.

IV. Connections to Third Party Networks

Any permanent connection intended to route traffic from theVijayranga Enterprises & Intermediaries (P)Ltd private network to a third party private network must have a business case documented and approved by the systems department

A risk analysis may be performed to ensure that the connection to the third party network will not compromise Vijayranga Enterprises & Intermediaries (P)Ltd's network. Controls, such as the establishment of firewalls and/or a DMZ (demilitarized zone), may be implemented between the third party and Vijayranga Enterprises & Intermediaries (P) Ltd to protect Vijayranga Enterprises & Intermediaries (P)Ltd's trusted networks. These connections may be periodically reviewed or tested by the systems department to ensure:

- The business case for the connection is still valid and the connection is still required;
- The security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.

This policy requires that connection to the Vijayranga Enterprises & Intermediaries (P) Ltd network be done in a secure manner to preserve the integrity of the Vijayranga Enterprises & Intermediaries (P)Ltd, data transmitted over that network, and the availability of the network. The security requirements for each connection will be assessed individually, and be driven by the business needs of the parties involved.

Only authorized Information Security or IT network staff will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events.

Third parties requesting permanent access to the Vijayranga Enterprises & Intermediaries (P)Ltd network must have an internal Vijayranga Enterprises & Intermediaries (P) Ltd sponsor develop a business case for the network connection. A Vijayranga Enterprises & Intermediaries (P)Ltd non-disclosure/non-access agreement must be signed by an authorized Vijayranga Enterprises & Intermediaries (P)Ltd representative and a duly appointed representative from the third party organization who is legally authorized to sign such an agreement.

This document, describing the business case and network connection requirements, must be submitted to the systems department. The systems department has final approval authority. Failure to sign this document by either party will result in the connection being disapproved.

17. Monitoring and Privacy

Vijayranga Enterprises & Intermediaries (P)Ltd has the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

Vijayranga Enterprises & Intermediaries (P)Ltd for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on devices under intimation to the user. This includes items such as files, e-mails, Internet history etc.

18. E-mail access

- Users should refrain from using private email servers from Vijayranga Enterprises & Intermediaries (P) Ltd Network. E-mail service authorized by the Vijayranga Enterprises & Intermediaries (P) Ltd and implemented by the systems department should only be used for all official correspondence.

- For personal correspondence, users may use the name-based e-mail ID assigned to them on the Vijayranga Enterprises & Intermediaries (P) Ltd authorized e-mail service.

- Electronic mail is inherently not secure and should not be used to transmit highly sensitive/confidential information, due to the security risks which include but are not limited to:

    - Vulnerability of messages to unauthorized access or modification

or denial of service;

- Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;
- Legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance; Implications of publishing externally accessible staff lists;

19. Access to Social Media

- Users should comply with all the applicable provisions under the Government Laws, while posting any data pertaining to the Vijayranga Enterprises & Intermediaries (P) Ltd on social networking sites.

- Users should adhere to "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, discrimination, harassment and other applicable laws. Users should report any suspicious incident as soon as possible to the Systems department

- User should always use high security settings on social networking sites and should not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful and should not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

20. Network Security Checking

Network vulnerability scans are conducted periodically on systems that are essential to supporting a process that is critical to Vijayranga Enterprises & Intermediaries (P) Ltd business and annually on all other systems. Appropriate tools to scan the network and to report vulnerabilities will be identified by the department and will be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

The vulnerability scanning process is followed and tested at all times to minimize the possibility of disruption to Vijayranga Enterprises & Intermediaries (P) Ltd networks by such reviews. Reports of exposures to vulnerabilities will be forwarded to the systems department for review.

The use of network vulnerability scanning tools by anyone other than, or authorized by, systems department is prohibited. Any vulnerability scanning from the Internet must be conducted exclusively by appropriately authorized and trained organizations.

21. Penetration and Intrusion Testing

All production computing systems that provide organization information to external parties, either directly or through another service that provides information externally

(such as the World Wide Web), may be subjected to penetration analysis and testing. It may be necessary for another organization, a suitably qualified evaluation team or authorized third party to attempt a live test to validate potential vulnerabilities. Such analysis and testing will be used to determine if:

- The application may be changed by anyone while in production;
- An authorized user may access the application and cause it to perform unauthorized tasks;
- An unauthorized user may access, destroy or change any data; or
- An unauthorized user may access the application and cause it to take inappropriate action.

Only authorized administrators may perform penetration testing and the system department must approve each test. Any other attempts to perform such tests or to determine how a system may change or behave under abnormal circumstances, whether successful or not, will be deemed an unauthorized access attempt and will result in disciplinary or legal action.

22. Portable Computing Devices and Information Media

Highly sensitive (confidential) data should never be in unencrypted format on portable computing devices and information media. Individuals requiring remote access to secure information should do so only via the VPN services provided by the systems department with completion of VPN use agreement.

Storage media used to backup and archive information must be secured to prevent compromise of confidentiality or integrity.

When using portable computing devices (e.g. laptops, smart phones, personal data assistants) to access information special care must be taken to ensure that device and information accessed by that device is not compromised (ie: unauthorized persons viewing information on the screen).When accessing databases containing confidential information the mobile device user must be careful to never save data to the local hard-drive or other mobile storage device.

Remote Access

Remote connection to Vijayranga Enterprises & Intermediaries (P)Ltd's networks is allowed only through a Virtual Private Network (VPN) maintained by systems department for administrative business use access when remote work-related business is an absolute necessity. The VPN application and terms of agreement require systems department and understanding of their responsibility to:

- Protect organization information by ensuring un authorized users are not allowed

Access to Vijayranga Enterprises & Intermediaries (P)Ltd Internal networks via the VPN;

- Maintain system security patches and anti-virus definitions;
- Secure the equipment used to accessVijayranga Enterprises & Intermediaries (P)Ltd information resources;
- Ensure noun encrypted highly sensitive (confidential) information resides on the device.

Connecting dial-up modems to workstations that are stand-alone or simultaneously connected to Vijayranga Enterprises & Intermediaries (P)Ltd's local area network or to another internal communication network is prohibited.

23. Operations Management

Responsibilities, processes and procedures should be established and documented for the management and operation of all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.

Operating procedures for all Vijayranga Enterprises & Intermediaries (P)Ltd administrative systems and applications should be documented and maintained. Operating procedures are treated as formal documents with changes authorized by the supervisor. Documented procedures are also prepared for housekeeping activities associated with information processing and communication facilities such as computer startup and shutdown procedures, back-up, equipment maintenance, computer room management and safety.

Changes to Vijayranga Enterprises & Intermediaries (P) Ltd administrative information processing facilities and systems must be authorized and controlled through a change management process with appropriate checks and balances. Formal management responsibilities and procedures ensure satisfactory control of all changes to equipment, software or procedural documentation. Operational software will be subject to strict change control. When programs are changed, an audit log containing all the relevant information will be created and maintained.
The change control process will consider the following activities:

- Identification and recording of significant changes;
- Assessment of the potential impact of the change;
- Formal approval process for proposed changes;
- Communication of changes to all affected people and organizations; and
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

24. Incident Management Procedures

An incident management process will be established to track the types, volumes and costs of security incidents and malfunctions. This information will be used to identify recurring or high impact incident sand to record lessons learned. This may indicate the need for

additional controls to limit the frequency, damage and cost of future incidents, or to be taken into account in the policy review process

All users of Vijayranga Enterprises & Intermediaries (P) Ltd systems should be made aware of the procedure for reporting security breaches, threats, weaknesses, or malfunctions that may have an impact on the security of Vijayranga Enterprises & Intermediaries (P) Ltd information. All Vijayranga Enterprises & Intermediaries (P) Ltd staff and contractors are required to report any observed or suspected incidents to local management as quickly as possible.

Incident management responsibilities and procedures will be clearly defined and documented to ensure a quick, effective and orderly response to security incidents. These procedures will address incidents such as:

- Information system failures and loss of service;
- Denial of service;
- Errors resulting from incomplete or in accurate business data;
- Breaches of confidentiality;
- Loss of integrity of the software or other system components.

In addition to normal contingency plans designed to recover systems or services, the incident response procedures will also cover:

- Analys is and identification of the cause of the incident;
- Planning and implementation of corrective actions to prevent reoccurrence;
- Collection of audit login formation;
- Communication with those affected by or involved in the recovery from the incident.

The systems department will investigate significant security incidents and implement corrective actions to reduce the risk of recurrence.

25. Segregation of Duties

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, should be implemented wherever possible, especially in support of the organisation's administrative systems.

Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that the security audit remains independent.

Care must be taken that no single person can perpetrate fraud in areas of single

Responsibility without being detected. The initiationofaneventmustbeseparatedfromits authorization.

Thefollowingcontrolsmustbeconsidered:

- Itisimportanttosegregateactivitieswhichrequirecollusioninordertodefraud, e.g.raisingasellorderforthesecuritiesandverifyingthattheproceedsis accounted;

If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

26. SeparationofTestandOperationalFacilities

Where possible, separating development, test and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status must be defined and documented

Development and test activities can cause serious problems, e.g. unwanted modificationof files or system environment, or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems must be considered to ensure adequate protection of the production environment. Where possible, a similar separation must also beimplemented between developmentandtestfunctions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems. Developers and testers also pose a threat to the confidentiality of operational information.

Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore required to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls must be considered:

- Developmentandoperationalsoftwaremust,wherepossible,runondifferent computer processors, or in different domains or directories;
- Developmentandtesting activitiesmustbeseparatedasfar aspossible;

Compilers,editorsandothersystemutilitiesmustnotbeaccessiblefrom operational systems when not required;

- Differentlog-onproceduresarerecommendedforoperationalandtestsystems,to reduce the risk of error. Users will be encouraged to use different passwords for these systems, and menus should display appropriate identification messages;

In situations whereseparate development and production support staff exist, development staff will only have access to operational passwords where controls are in place forissuing passwords for the support of operational systems. Controls must ensure that such passwords are changed after use.

27. SystemPlanningandAcceptance

Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. Requirements for new systems must be established, documented and tested prior to their acceptance and use.

Capacity demands should be monitored and projections of future capacity requirementsmadetoensurethatadequateprocessingcapabilityandstorageareavailable.This Information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Acceptance criteria based on best practices for new information systems, upgrades and new versions of existing systems must be established. Suitable tests will be performed to ensure requirements have been met prior to formal system acceptance, systemsdepartment will ensure that the requirements and criteria for acceptance are clearly defined, agreed, documented and tested.

28. ProtectionAgainstCode

Software and associated controls will be implemented across all Vijayranga Enterprises & Intermediaries (P) Ltd systems toprevent and detect theintroduction ofmalicious software. Theintroduction of maliciussoftwaresuchasacomputervirus,networkwormprogramsandTrojanHorses can cause serious damage to networks, workstations and business data.

User education will outline the dangers of unauthorized or malicious software. The types of controls and frequency of updating signature files, etc., is dependent on the value and sensitivity of the information that could be potentially at risk. For most Vijayranga Enterprises & Intermediaries (P) Ltdworkstations,andallsystemsorservers,virussignaturefilesareupdatedatleast daily.

29. InformationBack-up

Back-upsofcriticalVijayranga Enterprises & Intermediaries (P)Ltddataandsoftwareareperformedonadailybasis. A threat and risk assessment is performed at least annually to determine the criticality of businesssystems,andthetimeframerequiredforrecovery.Processeswillbedeveloped to back-up the data and software. Restoration of data is tested periodically. Formal disaster recovery plans for each critical Vijayranga Enterprises & Intermediaries (P) Ltd application will be developed, documented and tested periodically. Test results will inform changes to disaster recovery plans.

30. SystemSecurityChecking

Systems and services that process or store non-public information or provide support for critical processes will undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. ReviewsofsystemsandservicesthatareessentialtosupportingacriticalVijayranga Enterprises & Intermediaries (P) Ltd function must be conducted at least once every year.
Any deviations from expected or required results that are detected by the security status review process must be reportedto thesystemsdepartmentand corrected immediately. In addition, Vijayranga Enterprises & Intermediaries (P) Ltd application ownersshould beadvisedofthedeviations and must initiate investigation of the deviations (including the review of system activity log records if necessary).

31. Disposal ofMedia

Media such as tapes, diskettes, servers, mainframe and PC hard drives which contain sensitive data, must be disposed of in accordance with Law. Sensitive information could beleakedtooutsidepersonsthroughcarelessdisposalofmedia.Formalprocessesmustbe established to minimize this risk. Media containing sensitive Vijayranga Enterprises & Intermediaries (P) Ltd data must bedestroyed by incineration, shredding, or electronicerasureofdata beforedisposal consistent with record retention laws.

32. DataAccessControl

Systemsdepartmentsareresponsiblefordeterminingwhoshouldhaveaccesstoprotected resources within their jurisdiction, and what those access privileges will be (read, update, etc.).

Any Data User may request that a systems department review the restrictions placed on a

data element or data view, or review a decision to deny access to limited-accessdata. The departmentmakesthefinaldeterminationaboutrestrictionsandaccessrightsfor

enterprisedata.

Systems departments share security administration responsibilities (i.e., the functions of specifying, implementing, and managing system and data access control). To the extent possible, the system department works together with the database administrators to define a single set of procedures for requesting and authorizing access to limited-access data elements.

Systemsdepartmentsareresponsiblefordocumentingtheseaccessrequestsand

The System Department is responsible for defining and implementing procedures to assure that data are backed up and recoverable in response to events that could compromise data integrity.
The Information security program team formed by the system department is responsible for maintaining a plan for security policies and practices and for keeping abreast of security related issues internally within the organization community and externally throughout the information technology marketplace.

33. UserRegistrationandManagement

A process will be established to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals or other entities have access to Vijayranga Enterprises & Intermediaries (P) Ltd applications and information and that these users only have access to the resources required for authorized purposes.

TheUserManagementProcessshouldincludethefollowingsub-processes:

- Enrollingnewusers;
- RemovinguserIDs;
- Grantingprivilegestoauser;
- Removingprivilegesfroma user;
- Periodicreviewingofprivilegesofusers;
- Periodicreviewingofusersenrolledtoanysystem;and
- Assigninganewauthenticationtoken(e.g.passwordresetprocessing).

The appropriate authorized officer will make requests for the registration, granting, and revocation of access rights for all authorized users.

For applications that interact with individuals that are not employed, registered, or appointed by Vijayranga Enterprises & Intermediaries (P) Ltd, the information owner is responsible for ensuring an appropriate user management process is implemented where limitation of access is appropriate. Standards for the registration of such external users must be defined, to include the credentials that must be provided to prove the identity of the user requesting registration, validation of the request and the scope of access that may be provided.

34. UserPasswordManagement

Passwords are a common means of authenticating a user's identity to access an information system orservice. Password standardsareimplementedandcommunicated to ensure all authorized individuals accessing Vijayranga Enterprises & Intermediaries (P)

Ltd resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible.

35. SegregationofNetworks

When the Vijayranga Enterprises & Intermediaries (P) Ltd network is connected to another network, or becomes a segment on a larger network, controls are in place to prevent users from other connected networks from unauthorized access to sensitive areas of Vijayranga Enterprises & Intermediaries (P)Ltd‟s private network. Routers or other technologies are implemented to control access to secured resources on the trusted Vijayranga Enterprises & Intermediaries (P) Ltd network.

36. OperatingSystemAccessControl

Access to operating system code, services and commands must be restricted to only those individualswhoneed access inthenormal performanceoftheirorganization roles. Where possible, individuals will have a unique user ID for their use so that activities can be traced to the responsible person. Where avoidable, user IDs should not give anyindication of the user‟s privilege level, e.g., supervisor, manager, administrator.

In certain circumstances, wherethereis a clearbusiness requirement orsystem limitation, the use of a shared user ID for a group of users or a specificjobcan beused. Approval by management should be documented in these cases. Additional compensatory controls must be implemented to ensure accountability is maintained.

ApplicationAccessControl

Access to Vijayranga Enterprises & Intermediaries (P) Ltd applications must be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems must berestricted. This access should be further restricted so that authorized Vijayranga Enterprises & Intermediaries (P) Ltd staff and contractors can access only thoseapplications and systems they directly support.

Monitoring System Access and Use Sensitive systems and applications are monitored to detect deviation from the access control policy and record events to provide evidence and reconstruct lost or damaged data. Depending on the nature of the events continuous and/or periodic monitoring may be appropriate.
Audit logs recording exceptions and other security-relevant events that represent security incidents/deviations from policy are produced and kept to assist in future investigations and access control monitoring.

Auditlogswillincludewheretechnicallyfeasible:

- UserIDs;
- Datesandtimesforlogonandlogoff;

- Terminalidentityorlocationifpossible;
- Recordsofrejectedsystemaccessattempts;and
- Recordsofrejecteddataandotherresourceaccessattempts.

37. SystemsDevelopmentandMaintenance

Software applications are developed or acquired to support Vijayranga Enterprises & Intermediaries (P) Ltd in achieving its mission. These applications generally store, manipulate, retrieve and display information used to conduct Vijayranga Enterprises & Intermediaries (P) Ltd activities. Vijayranga Enterprises & Intermediaries (P) Ltd departments and customers becomedependentontheseapplications,anditisessential the data processed by these applications be accurate, and readily available for authorized use. It is also critical that the software that performs these activities be protected from unauthorized access or tampering.

To ensure that appropriate security is built into all Vijayranga Enterprises & Intermediaries (P) Ltd information systems, all security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for a Vijayranga Enterprises & Intermediaries (P) Ltd information system.

Security requirements and controls must reflect the value of the information assets involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Web and other online applications. Theframework for analyzing the security requirements and identifying controls to meet them is associated with threat assessment and risk management which must be performed bythe information owner and technical support staff.

Aprocessmustbeestablishedandimplementedforcriticalapplicationsto:

- Understandthebusinessrisksanddevelopaprofileofthedatatohelpto understand the risks;
- Selectsecuritymeasuresbasedontheriskprofileandprotection requirements;
- Selectandimplementspecificcontrolsbasedonsecurityrequirementsand technical architecture;
- Provideamethodtotesttheeffectivenessofthesecurity controls;
- Developprocessesandstandardstosupportchanges,ongoingmanagementandto measure compliance.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level. At a minimum, the security measures that are implemented must be based on the threat and risk assessments of the information being processed.

38. InputDataValidation

Datainput must bevalidated.Checks will beappliedto theinput ofbusiness transactions,

staticdata(names,addresses,employeenumbers,etc.)andparametertables.Where

feasible the applications should apply the controls as part of the system to ensure consistent, complete, and accurate implementation of the controls in the most efficient manner.

Thefollowingcontrolsmustbeconsidered:
Dualinputorotherinputcheckstodetectthefollowing errors:

- Out-of-rangevalues;
- Invalidcharactersindatafields;
- Missingorincompletedata;
- Exceedingupperandlowerdatavolumelimits;
- Unauthorizedorinconsistentcontroldata.

ValidationoftheinputscompliancewithVijayranga Enterprises & Intermediaries (P)Ltdpolicy,proceduresand business rules.

- Periodicreviewofthecontentofkeyfieldsordatafilestoconfirmtheirvalidity and integrity;
- Inspectinghard-copyinputdocumentsforanyunauthorizedchangestoinput data (all changes to input documents should be authorized);
- Proceduresforrespondingtovalidationerrors;
- Proceduresfortestingtheplausibilityoftheinputdata;
- Definingtheresponsibilitiesofallpersonnelinvolvedinthedatainput process.

39. ControlofInternalProcessing

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks and business rules must be incorporated into systems andautomatedwherepossible.Thedesignofapplicationsmustensurethatrestrictionsare implemented to minimize the risk of processing failures leading to a loss of data orsystem integrity.
Specificareastoconsiderinclude:

- Theuseandlocationinprogramsofaddanddeletefunctionstoimplement change to data;
- Theprocedurestopreventprogramsrunninginthewrongorderorrunningafter failure of prior processing;
- Theuseofcorrectionprogramstorecoverfromfailurestoensurethecorrect processing of data.
- Useofautomatedcheckingonthedatabase(triggers)toensurekeyvalidation rules are applied at the database level.

40. CryptographicControls

Use of cryptography for protection of high-risk information must be considered when other controls do not provide adequate protection. Encryption is a technique that can be used to protect the confidentiality of information. It must be considered for the protection of sensitive or critical information. Based on a risk assessment, the required level of protection will be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys employed.

To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration must be given to controls that apply to the export and import of cryptographic technology.

KeyManagement

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. Asecuredenvironmentmustbeestablishedtoprotectthecryptographickeysused to encrypt and decrypt information. Access to these keys must be tightly controlled to only thoseindividualswhohaveabusinessneedtoaccessthekeys.Lossofconfidentialityofa cryptographic key would cause all information encrypted with that key to be considered compromised.

ChangeControlProcedures

To minimize the possibility of corruption of administrative information systems, strict controls over changes to information systems must be implemented. Formal change control procedures must be enforced. They must ensure that security and control proceduresarenot compromised,thatsupportprogrammersaregivenaccessonlytothose parts of a system necessary to perform their jobs, andthatformalagreement and approval processes for changes are implemented.

These change control procedures will apply to Vijayranga Enterprises & Intermediaries (P) Ltd applications as wellas systems software used to maintain operating systems, network software, hardware, etc.

In addition, access to source code libraries for both Vijayranga Enterprises & Intermediaries (P) Ltd applications and operating systems must be restricted to ensure that only authorized individuals haveaccess to theselibraries and whereпractical that access is loggedto ensure all activity can be monitored.

41. SafeguardingofVijayranga Enterprises & Intermediaries (P)Ltd Records

Vijayranga Enterprises & Intermediaries (P) Ltd records must be protected from loss, destruction or unauthorized modification. Some records may need to be retained in a

secure manner for extended periods to meet SEBI, stock exchange retention requirements, as well as to support essentialbusinessoperations.Recordsandinformationmustbecategorizedintorecord

types,e.g.,accountingrecords,databaserecords,transactionlogs,auditlogs,and operational procedures, each with details of retention periods and types of storage media.

CYBERSECURITYANDCYBERRESILIENCEPOLICY

Ref:SEBIcircularNo.SEBI/HO/MIRSD/CIR/PB/2018/147

1. StatutoryMandate

ThisframeworkisformedinaccordancewiththerequirementsoftheSEBICircular-SEBI/HO/MIRSD/CIR/PB/2018/147 ("the circular") dated December 3, 2018.

Rapid technological developments in the securities market have highlighted the need for maintaining a robust cyber security and cyber resilience framework to protect the integrity ofdata and guard against breaches of privacy. Since stock brokers perform significant functions in providing services to theirclients, it is desirablethat these entities have robust cybersecurity and cyber resilience framework in order to provide essential facilities and perform systemically critical functions relating to the securities market.

2. Objective

The objective of this framework is to provide robust cyber security and cyber resilience to the Stockbrokers and depository participants to perform their significant functions in providing services to the holders of securities.

Toimplementtheaboveframework,aTechnologyCommitteeisformedcomprisingoffollowing individuals:

Sl.No	Name	Designation	Positionin Committee
1	Mr.KrishnanVaidyanathanHariharaNurani	Director	Chairman
2	Mr.PramodGJain	WholeTime Director	Member
3	Mr.JineshCK	Manager, SystemsDepartment	Member

Mr.JineshCKshallberesponsibleforDesignatedOfficerfordefiningandimplementationof this framework.

3. Applicability

Provisionsofthesaidcircularandframingofcybersecurityandcyberresiliencearerequiredtobe complied by all Stock Brokers and Depository Participants registered with SEBI. The policy has been considered, taken on record and approved by the board of directors of the company at their duly convened meeting held on January 10,2025.

4. Scope

Cyber-attacks and threats attempt to compromise the Confidentiality, Integrity and Availability (CIA)ofthecomputersystems,networksanddatabases(Confidentialityreferstolimitingaccess ofsystemsand informationtoauthorizedusers,Integrityistheassurancethattheinformationis reliable and accurate, and Availability refers to guarantee of reliable access to the systems and information by authorized users).

Cybersecurityframeworkincludesmeasures,toolsandprocessesthatareintendedtoprevent

cyber-attacksandimprovecyberresilience.CyberResilienceisanorganization'sabilitytoprepare and respond to a cyber-attack and to continue operation during,and recover from, a cyber-attack.

With the view to strengthen and improve Cyber Security and Cyber Resilience framework, the board of directors of the company shall review this policy documents and implementation thereof at least once annually.

5. Identification,AssessmentAndManagementOfCyber Security Risk

IDENTIFICATION

Thecommitteeanddesignatedofficershallidentifythecriticalassetsbasedontheirsensitivityand criticality for business operations, services and data management including various servers, data processing systems, and information technology (IT) related hardware and software etc.

The IT team shall maintain up-to-date inventory of its hardware and systems and the personnel to whomthesehavebeenissued,softwareandinformationassets(internalandexternal),detailsofits network resources, connections to its network and data flows.

PROTECTION

Inordertoprotectthecybersafety,thecompanyshallensurethemeasureswhichinclude,however not limited up to:

- Accesscontrols
- PhysicalSecurity
- NetworkSecurityManagement
- Datasecurity
- HardeningofHardwareandSoftware
- ApplicationSecurityinCustomerFacingApplications
- Certificationofoff-the-shelfproducts
- Patchmanagement
- Disposalofdata,systemsandstoragedevices
- VulnerabilityAssessmentandPenetrationTesting (VAPT)

No unauthorized person, irrespective of his/her designation, post or rank should have the right to access critical systems, confidential data, applications or facilities. Password Policy is made mandatory for all levels of data access with sufficient complexity of the Password placed.

Any access given shall be for a defined period and defined purpose only. Vijayranga Enterprises & Intermediaries (P) Ltd shallgrant access to IT systems, applications, databases and networks on a need-to-use basis and based on the principle of least privilege. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.

The access to the IT systems, applications, databases and networks needs to be sent on mail approved by immediate superior.

Two Factor Authentication shall also be implemented across the applications in a phasedmanner. Passwords, security PINs etc shall be stored in an encrypted manner in one way hashed encryption using cryptographic hash functions.

After Five (5) failed login attempts into Applications, the Customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed via an out-of-band channel validation, for instance, a cryptographically secure unique link that is sent to the Customer's registered email, a random OTP (One Time Password) that is sent as an SMS to the Customer's registered mobile number, or manually by Vijayranga Enterprises & Intermediaries (P)Ltd after verification of the Customer's identity etc.

Vijayranga Enterprises & Intermediaries (P) Ltd shall also ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes. Such logs shall be maintained for a period of minimum two years.

Vijayranga Enterprises & Intermediaries (P) Ltd shall formulate an Internet access policy to

monitor and regulate the use of internetandinternet-basedservicessuchassocialmediasites,cloud-basedinternetstoragesites,

etc.withinthecritical IT Infrastructure.

The IT team shall also address deactivation of access privileges of users who are leaving the organization or whose access privileges have been withdrawn.

DETECTION

Necessary steps as may be required to monitor and for early detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmissionofdataheldincontractualorfiduciarycapacity,byinternalandexternalpartiesshall be maintained, appreciated and taken care of.

The security logs of systems, applications and network devices exposed to the internet shall also be,from time to time, monitored for anomalies, if any. The companyshall ensurehighresilience, highavailabilityandtimelydetectionofattacksonsystemsandnetworksexposedtotheinternet, and implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet.

6. ResponseandRecovery

Alerts generated from monitoring and detection systems should be suitably investigated in order to determine activities that are to be performed to prevent expansion of such incidents of cyber attack or breach, mitigate its effect and eradicate the incident.

The response and recovery plan should have plans for the timely restoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternate services or systems to Customers. Team shall ensure that we have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as specified by SEBIfor Market Infrastructure Institutions vide SEBI circular CIR/MRD/DMS/17/20 dated June 22, 2012 as amended from time to time.

Any incident of loss ordestruction ofdataorsystems should bethoroughly analyzed and lessons learned from such incidents should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

With a view to providing quick responses to such cyber-attacks, the committee shall formulate a responseplandefiningresponsibilitiesandactionstobeperformedbyitsemployeesand support

/outsourced staffintheeventofcyber-attacksor breachofCyberSecuritymechanism.Suchplan andanymodificationthereinshallbecirculatedamongstalltheemployeesandsupport/

outsourcedstafffromtimetotime.

7. **CommunicationOfUnusualActivitiesAndEvents**

The systems department of the company under guidance of the committee shall monitor unusual activities and events and shall facilitate communication of the same to designated officers for necessary actions, as may be required.

RESPONSIBILITIESOFEMPLOYEES,MEMBERSANDPARTICIPANTS

Inadditiontothefollowing,theemployees,membersandparticipantsshallberesponsibleforthe dutiesandobligationsasmaybeentrustedandcommunicatedbythecompany/committee /designatedofficerfrom timeto time.

Topreventthecyberattacks,theemployees,membersand participants shall assist the companyto mitigate cyber attacks by adhering the followings:

- To attend the cyber safety and training programs as conducted by the company fromtime to time.
- Toendureinstallation,usageandregularupdateofantivirusandantispyware softwareon computers used by them.
- UseafirewallforyourInternetconnection.
- Downloadandinstallsoftwareupdatesforyouroperatingsystemsandapplications asthey become available.
- Makebackupcopiesofimportantbusinessdataandinformation.
- Controlphysicalaccesstoyourcomputersandnetworkcomponents.
- KeepyourWi-Finetworksecuredandhidden.
- To adhere to limited employee access to data and information andlimitedauthorityto install software.
- Regularlychangepasswords.
- Donotuseorattachunauthorizeddevices.
- Donottrytoopenrestricteddomains.
- Avoidsavingyourpersonalinformationonthecomputeroranyfinancialdataonany authentic website.
- Togetyourcomputerregularlyscannedwithanti-virussoftware.
- Donotreleasesensitivedataoftheorganization.
- No person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities.
- Any access to the systems, applications, networks, databases, etc., shall be for a defined purpose and for a defined period. The company shall grant access to IT systems, applications,databases and networks on a need-to-use basis and based on the principle of least privilege. Such access shall be for the periodwhen the access is required and should

beauthorizedusingstrongauthenticationmechanisms.

- An access policy which addresses strong password controls for users' access to systems, applications, networks and databases shall be implemented.
- All critical systems accessible over the internet should have two-factor security (such as VPNs, Firewall controls etc.), as far as possible.
- The company shall ensure that records of user access to critical systems, wherever possible, are uniquely identified and logged for audit and review purposes and such logs wouldbemaintainedandstoredinasecurelocationforatimeperiodnotlessthantwo (2)years.
- Thecompanyshallberequiredtodeploycontrolsandsecuritymeasurestosupervisestaff with elevated system access entitlements (such as admin or privileged users) to company'scriticalsystems.Suchcontrolsandmeasuresshallinter-aliaincluderestricting the numberofprivileged users,ifany,periodic review of privileged users' activities, disallowprivilegedusersfrom accessing systems logs in which their activities are being captured, strong controls over remote access by privileged users, etc.
- Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, shall be subject to stringent supervision, monitoring and access restrictions.
- An Internet access policy to monitor and regulate the use of internet and internet based services such as social media sites, cloud-based internet storage sites, etc. within the company's critical IT infrastructure shall be formulated.
- User Management shall address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn.
- Physical access to the critical systems shall be restricted to minimum and only to authorized officials. Physical access of outsourced staff / visitors shall be properly supervisedbyensuringat theminimum that outsourced staff/ visitors areaccompanied at all times by authorized employees.
- Physical access to the critical systems shall be revoked immediately if the same is no longer required.
- The company will ensure that the perimeter of the critical equipment room, if any, shall be physically secured and monitored by employing physical, human and procedural controls such as the use of security guards, CCTVs, card access systems, mantraps, bollards, etc. where appropriate.
- The company shall establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within their IT environment. The LAN and wireless networks shall be secured within the premises with proper access controls.
- For algorithmic trading facilities, adequate measures shall be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications, if any.
- The company shall install network security devices, such as firewalls, proxy servers, intrusion detection and prevention systems (IDS) to protect their IT infrastructure which is exposed to the internet, from security exposures originating from internal and external sources.

- Adequate controls shall be deployed to address virus / malware / ransom ware attacks. These Controls may include host / network / application based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.
- Critical data shall be identified and encrypted in motion and at rest by using strong encryption methods. Illustrative measures in this regard are given in Annexure A and B.
- The company shall implement measures to prevent unauthorized access or copying or transmissionofdata/informationheldincontractualorfiduciarycapacity.Itshallensure that confidentiality of information is not compromised during the process of exchanging and transferring information with external parties.
- This security policy also covers use of devices such as mobile phones, faxes,photocopiers ,scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.
- The company shall allow only authorized data storage devices within their IT infrastructure through appropriate validation processes.
- The company shall only deploy hardened hardware / software, including replacingdefault passwords with strongpasswords and disabling orremoving services identified as unnecessary for the functioning of the system.
- Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures taken to secure them.
- Application security for Customer facing applications offered over the Internet such as IBTs(Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personalinformation offered by Brokers to Customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use. Required measures for ensuring security in such applications shall be ensured.
- The company shall ensure that off the shelf products, if any, being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4. The Common criteria certification in India is being provided by(STQC) Standardization Testing and Quality Certification (Ministry of Electronics and Information Technology). Custom developed / in-house software and components need not obtain the certification, but have to undergo intensive regression testing, configuration testing etc. The Scope of tests shall include business logic and security controls.
- The company establishes and ensures that the patch management procedures include the identification, categorization and prioritization of patches and updates. An implementation timeframe for each category of patches should be established to apply them in a timely manner.
- The company shall perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
- Suitable policy for disposal of storage media and systems shall be framed as may be required. The critical data/ Informationon such devices and systemsshallberemovedby using methods such as crypto shredding / degauss / Physical destruction as applicable.

- The company shall formulate a data-disposal and data-retention policy to identify the value and lifetime of various parcels of data.
- The company shall regularly conduct vulnerability assessment to detect security vulnerabilities in their IT environments exposed to the internet, as and when required.
- The company with systems publicly available over the internet shall also carry out penetration tests, at-least once a year, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on its systems and networks that are exposed to the internet. In addition, the company shall perform vulnerability scanning and conduct penetration testing prior to the commissioning of a new system that is accessible over the internet.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applicationsprovidedby exchangeempanelledvendors,thecompanyshallreportthemto the vendors and the exchanges in a timely manner.
- Remedial actions, if required, shall be immediately taken to address gaps that are identified during vulnerability assessment and penetration testing.
- The company shall establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet shall also be monitored for anomalies, if any.
- Further, to ensure high resilience, high availability and timely detection of attacks on systems and networks exposed to the internet, the company shall implement suitable mechanisms to monitor capacity utilization of its critical systems and networks that are exposed to the internet, for example, controls such as firewalls to monitor bandwidth usage.
- Alerts, if any, generated from monitoring and detection systems shall be suitably investigated in order to determineactivitiesthataretobeperformedtopreventexpansion of such incident of cyber attack or breach, mitigate its effect and eradicate the incident.
- The response and recovery plan of the company shall have plans for the timelyrestoration of systems affected by incidents of cyber-attacks or breaches, for instance, offering alternative services or systems to Customers. The company shall have the same Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per regulatory requirements.
- Responsibilities and actions to be performed by company's employees and support / outsourced staff in the event of cyber-attacks or breach of Cyber Security mechanism shall be defined.
- Any incident of loss or destruction of data or systems shall be thoroughly analyzed and lessons learned from such incidents shall be incorporated to strengthen the security mechanism and improve recovery planning and processes.
- Suitable periodic checks to test the adequacy and effectiveness of the aforementioned response and recovery plan shall be done.

8. SubmissionOfQuarterlyReports

Quarterly reports containing information on cyber-attacks and threats experienced, if any, by the company and measures taken to mitigate vulnerabilities, threats and attacks includinginformation on bugs / vulnerabilities / threats that may be useful for other Stock Brokers / Depository Participants shall be submitted to Stock Exchanges / Depositories, as per statutory requirements /guidelines.

9. TrainingandEducation

We shall work on building Cyber Security and basic system hygiene awareness of staff (with a focus on staff from non-technical disciplines). We shall also conduct periodic training programs to enhance knowledge of IT / Cyber Security Policy and standards among the employees incorporating up-to-date Cyber Security threat alerts. The training programs should be reviewed and updated by team to ensure that the contents of the program remain current and relevant.

10. Systemsmanagedbyvendors

Where the systems (Back office and other Customer facing applications, IT infrastructure, etc.) are managed by vendors and due to which we shall not be able to implement some of the aforementioned guidelines directly, we shall instruct the vendors to adhere to the applicable guidelines in the Cyber Security and Cyber Resilience policy and obtain the necessary self-certifications from them to ensure compliance with the policy guidelines**.**

11. SystemsManagedByMiIIs

Wherever the applications are offered to customers over the internet by MIIs (Market Infrastructure Institutions), for eg.: NSE's NOW, BSE's BEST etc., the responsibility ofensuring Cyber Resilience on those applications reside with the MIIs and not with the company. In such case, the company is exempted from applying the aforementioned guidelines to such systems offered by MIIs such as NOW, BEST, etc

12. PERIODICAUDIT

The company shall arrange to have its systems audited on an annual basis by a CERT-IN empanelledauditororanindependentDISA/CISA/CISMqualifiedauditortocheckcompliance withtheaboveareas and shallsubmitthereporttoStockExchanges/Depositoriesalongwiththe commentsoftheBoard/ committee/anycommitteethereofwithinthreemonthsoftheendofthe financial year.

Password
Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Vijayranga Enterprises & Intermediaries (P)Ltds entirecorporate network. As such, all Vijayranga Enterprises & Intermediaries (P)Ltdemployees(includingcontractors and vendors with access to Vijayranga Enterprises & Intermediaries (P) Ltd are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequencyof change.

Policy

1. Allsystem-levelpasswords(e.g.,root,enable,admin,applicationadministration accounts, etc.) must be changed at least twice on a quarterly basis.
2. Allproductionsystem-levelpasswordsmustbepartoftheVijayranga Enterprises & Intermediaries (P)Ltd administered global password Management database.
3. Alluser-levelpasswords(e.g.,email,web,desktopcomputer,etc.)mustbechanged at least every three months.
4. Useraccountsthathavesystem-levelprivilegesgrantedthroughgroupmemberships orprogramsmusthavea uniquepasswordfromall otheraccountsheldbythatuser.
5. Passwordsmustnotbe inserted into email messages or other forms of electronic communication.
6. Alluser-levelandsystem-levelpasswordsmustconformtotheguidelinesdescribed below.

Guidelines

PasswordsareusedforvariouspurposesatVijayranga Enterprises & Intermediaries (P)Ltd.Someofthemorecommonuses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamicpasswords whichareonly usedonce),everyoneshould beaware ofhowto selectstrong passwords.

Poor,weakpasswordshavethefollowingcharacteristics:

- ✔Thepasswordcontainslessthanorequaltofifteencharactersandgreaterthanor equal to six characters
- ✔Thepasswordisawordfoundinadictionary (Englishor foreign)

✔Thepasswordisacommonusagewordsuchas:Namesoffamily,pets,friends, co-workers, fantasy characters, etc.

✔Computertermsandnames,commands,sites,companies,hardware,software.

✔Thewords"BgSE","securities"orany derivation.

✔Birthdaysandotherpersonalinformationsuchasaddressesandphonenumbers.

✔Wordornumberpatternslikeaaabbb,qwerty,zyxwvuts,123321,etc.

✔Anyoftheabovespelledbackwards.

✔Anyoftheabovepreceded orfollowedbyadigit(e.g.,secret1,1secret) Strong passwords have the following characteristics:

✔Containbothupperandlowercasecharacters(e.g.,a-z,A-Z)

✔Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\` {}[]:";'<>?,./)

✔ Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).

✔Arenotwordsinanylanguage,slang,dialect,jargon,etc.

✔Arenotbasedonpersonalinformation,namesoffamily, etc.

✔ Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE:Donotuseeitheroftheseexamplesas passwords!

B.PasswordProtectionStandards

Do not use the same password for Vijayranga Enterprises & Intermediaries (P) Ltdaccounts as for other non Vijayranga Enterprises & Intermediaries (P) Ltd access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Vijayranga Enterprises & Intermediaries (P) Ltdaccess needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account. Do not share Vijayranga Enterprises & Intermediaries (P) Ltd with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Vijayranga Enterprises & Intermediaries (P) Ltd information. Here is a list of "don'ts":

✔Don'trevealapasswordoverthephoneto ANYONE

✔Don'trevealapasswordinanemail message

✔Don'trevealapasswordtotheboss

✔Don'ttalkaboutapasswordinfrontofothers

✔Don'thintattheformatofapassword(e.g.,"myfamily name")

✔Don'trevealapasswordonquestionnairesorsecurity forms

✔Don'tshareapasswordwithfamily members

✔Don'trevealapasswordtoco-workerswhileonvacation.

If someone demands a password, refer them to this document or have them call someone in the InformationSecurityDepartment.Donotuse the "RememberPassword" featureofapplications. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended changeinterval is everyfourmonths. If an account or password is suspected to have been compromised, report the incident to Vijayranga Enterprises & Intermediaries (P) Ltd s and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Vijayranga Enterprises & Intermediaries (P) Ltdor its delegates. If a password is guessed or cracked during one of these scans,the user will be required to change it.

C.ApplicationDevelopmentStandards

Applicationdevelopersmustensuretheirprogramscontainthefollowingsecurityprecautions.
Applications:

✔Shouldsupportauthenticationofindividualusers,not groups.

✔Shouldnotstorepasswordsincleartextorinanyeasilyreversibleform.

✔Shouldprovideforsomesortofrolemanagement,suchthatoneusercantakeover the functions of another without having to know the other's password.

D.UseofPasswordsandPassphrasesforRemoteAccessUsers

Access to the Vijayranga Enterprises & Intermediaries (P) LtdNetworksviaremoteaccessistobecontrolledusingeithera one-time password authentication or a public/private key system with a strong passphrase.

4.6 Enforcement

Any employee found to have violated this policy may besubject to disciplinary action, up to and including termination of employment.

Annexure-3-BackupPolicy

Back-up copies of essential business information and software will be taken on a daily basis. Adequate back-up facilities must be provided to ensure that all essential business informationand software can be recovered following a disaster or media failure.

- Aminimum level ofback-up information, togetherwith accurate and completerecordsof the back-up copies and documented restoration procedures, must be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information will be retained for important business applications.

- Back-up information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site must be extended to cover the back-up site.
- Back-up media must be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

- Restoration procedures must be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational proceduresforrecovery.Theretentionperiodforessentialbusinessinformation,andalso any requirement for archive copies to be permanently retained, must be determined.

Backup

- CopyalltheabovebackupsintheExternalTape Drives.
- Putcopiestothreedifferentcomputersinthesamenetwork.
- KeeponecopyofbackupinHO,sendsecondcopytoSecondarylocation trusted by the company to be safe enough to securely house th e backup of data
- ThirdonetakentoManagingDirector'sResidence
- MaintainingBackupRegister.

Restoreprocedure

- AbovegivenbackupsarerestoredtothebackupserverusingBackup&Restore utility on a daily basis.
- Testingbackupserveronmocktradingsession

Backupforflawlesstradingnetwork

1. HavealeasedlinetoNSEwithadoublelockingfacilitywithVSAT.Iftheleasedline goes down use the VSAT as backup.
2. HaveBackupManager/RAPIDserverforCTCLserver backup.
3. Have1:1,100MbpsAirtelInternetConnectionasBackupforTATA1:1,30Mbps Leased Line connection for Internet Trading.
4. BackupFirewall(Netgear)forInternettrading.
5. DedicatedNSEVSATatChennaiOfficeforbackuptradingoverphone.
6. DisasterrecoverysiteatCtrlSdatacenter,Mumbai

Annexure-4

BusinessContinuityPlanning

A. The scope of this policy is limited to the IT infrastructure, and the data and applications of the local Vijayranga Enterprises & Intermediaries (P) Ltd environment. To ensure interruptions to normal Vijayranga Enterprises & Intermediaries (P) Ltd business operations are minimized, and critical trading business applications and processes are protected from the effects of major failures or disasters, each Vijayranga Enterprises & Intermediaries (P) Ltd business unit, in cooperation with the Vijayranga Enterprises & Intermediaries (P) Ltd IT organization, must develop, implement and periodically test a local business continuity plan that can meet the recovery requirements of all critical business processes and applications. These interruptions could be caused by natural disasters, accidents, equipment failures, or deliberate actions.

The consequences of an extended interruption due to a disaster or security failure must be analyzed to determine the impact on Vijayranga Enterprises & Intermediaries (P)Ltd‟s business, and to determine the recovery time necessary to restore normal business operations. Business continuity management must include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

Businesscontinuitymanagementbeginswithabusinessimpactanalysisandathreatanalysis that identifies events that could cause an interruption of business operations and processes. Following the threat identification, a risk assessment must be performed to determine the impactofthethreatonthebusiness,likelihoodofoccurrence,andrecoverytimenecessaryfor essential Vijayranga Enterprises & Intermediaries (P) Ltd business applications and processes. This assessment will consider only those business processes that are information technology related. These activities must be performed with the full involvement of the owners of the business data and business processes.

AbusinesscontinuityplanmustbedevelopedbyeachVijayranga Enterprises & Intermediaries (P)Ltdbusinessunitthat addresses each of the following key elements:

- Understanding the risks Vijayranga Enterprises & Intermediaries (P) Ltd is facing in terms of their likelihood and impact on the business, including identification and prioritization of businessprocesses and supporting applications;

- Understanding the impact the interruptions are likely to have on Vijayranga Enterprises & Intermediaries (P) Ltd, and establishing the business objectives of information processing facilities;

- Formulating and documenting a business continuity strategy and plans that areconsistentwithVijayranga Enterprises & Intermediaries (P)Ltd‟sbusinessobjectivesandpriorities;

Regulartestingandupdatingofthebusinesscontinuityplansandprocessesthathavebeenput in place;

- EnsuringthatthemanagementofbusinesscontinuityisbuiltintoVijayranga Enterprises & Intermediaries (P)Ltd‟s processes and structure. Responsibility for coordinating the business continuity management process should be assigned to appropriate individuals.

- ForallinstanceswhereVijayranga Enterprises & Intermediaries (P)Ltdisreliantupontheservicesofathirdparty for providing information services,Vijayranga Enterprises & Intermediaries (P) Ltd will define the requirements for information availability and recovery. These requirements must be made part ofthe agreement with the party providing services.

Althoughinformationsecurityrolesandresponsibilitiesmaybeoutsourcedtothirdparties,it istheoverallresponsibilityofeachVijayranga Enterprises & Intermediaries (P)Ltdbusinessunittomaintaincontrolof the security of the information assets that it owns.

The disaster recovery requirements for the Information Technology (IT) components are based on the business impact analysisperformed byVijayranga Enterprises & Intermediaries (P) Ltd businessunitsand academic departments.

CLIENT CODE MODIFICATION

ErrorPolicyonClientCodeModification

1. Themodificationtotheclientcodeistobedoneonlyinexceptionalcasesandnot asaroutine one.

2. Thereasonformodificationhastobeascertainedandanalyzedandgenuinenessistobeestablished and also its impact on the clients should be studied before the modification.

3. Normallyasaprinciple,wearepermittedtochange clientcodesofnon-institutionalclientsonlyfor the following objective criteria;

   a. Errorduetocommunicationand/orpunchingortypingsuchthattheoriginalclientcode/name and the modified client code/name are similar to each other.

   b. Modificationwithinrelatives(Relativeforthispurposewouldmean„Relative"asdefinedunder sec.2(77)theCompaniesAct,2013)

4. AClientCodeasdesignatederroraccountwillbeopenedwithnomenclature-Vijayranga Enterprises & Intermediaries (P)Limited- ERROR Account in the UCC database of the Exchange for the account which is classified as error account.

5. WewillinformtherespectiveExchange,byendofday,thereasonsformodificationofclient codes of non- institutional trades based on the aforesaid objective criteria.

6. Thereforeitisimperativethattheissueshouldbereportedtothe ComplianceOfficerandChief Executive Officer/Director and only with approval of Chief Executive Officer/Director, the modificationshouldbe carriedafterbeing satisfied thatitis genuine,the same is requiredtobe done to protect the interests of the client.

7. HencethefacilitytomodifytheclientcodesshouldbeavailableonlyattheCorporateManagerlevel and should not be given to the branches/Authorised Person.
8. Training program should be conducted to all the Dealers/Staffs and they should be explained how codemodificationscanbemisusedandwhatstepsshouldbetakentoavoidthesame.Italsoshould be explained that code modifications should not be encouraged to the clients except for cases like "punching errors/typing errors".

INTERNALCONTROL POLICIES

POLICYOFINTERNALCONTROLSYSTEM

Introduction

Vijayranga Enterprises & Intermediaries (P) Limited (hereinafter referred to as the 'COMPANY') a body corporate , registeredundertheprovisionsoftheCompaniesAct1956,isaSEBIregisteredbrokerofthe BombayStockExchangeofIndiaLtd.(BSE).Thecompanyhasadoptedvariouspolicies&procedure sforinternalcontrol measures&toolsforcomplianceofvariousActs,rules&regulationsoftheExchanges.

A. COMMENCEMENTOFBUSINESS

1. PhysicalreceiptofRegistrationCertificateasAuthorisedPersonfrom Exchangeis mandatorytostartbusinessasaAuthorisedPerson.
2. ThereshouldnotbeanyInvestorComplaintpendingagainstthatAuthorisedPersonin Company/Exchange/SEBI.Furtherthereshouldnot beanyArbitration/Legal case pendingagainstthat AuthorisedPersonintheCompany/Exchange/SEBI.
3. FollowingrequirementsaretobefulfilledbyanAuthorisedPersonbeforestartingthe business:
    a. BaseMinimumCapitaltobedepositedasseparatedepositintheformof cash with Company.
    b. ABeneficiaryAccountinDPistobeopened.
    c. ComplianceOfficerandPrincipalOfficerunderPMLAistobeappointed.

B. CLIENTREGISTRATION

New account opening form containing Rights and obligation documents, Risk Disclosure Document, Guidance for DO's and Don'ts for trading on Exchange, Policies & Proceduremust besigned by theclient. The client mayormaynot sign theVoluntary documents.

1. ThereshallnotbeanydirectClientsfortheCompany.UnderTripartiteAgreement, Clientwillbeentertainedandregisteredonlythroughanyofourregistered AuthorisedPerson.

   Itwillbemandatoryforeverypersontogethimself/herself/itselfregisteredas clienttostarttradingandtofillClientRegistrationForminlatestprescribedformatof theExchange/SEBIand details of all clients are to be uploaded/downloaded asthe casemaybewithKRAagency.

2. Pre-numbered Client Registration Forms duly filled and signed by Client, AuthorisedPersonandCompanyaretobekept insafecustodyalongwithnecessary documentsobtainedi.e.PANProof,AadharCard,ProofofIdentity,Address,DP anddetailsofBankAccount,TelephoneNumbers,EmailIDsetc.andonecopyoff alldocumentsistobesenttoKRAalsoinsoftform.

3. ClientshouldcomepersonallytoKYCDepartmentandOfficialsofCompanyshould verifythePANProof,DPProof,IDProof,addressproofwithOriginal.Incaseof the Outstation Clients, they shouldvisittonearby InvestorCentreofBFSLand OfficeInchargeofthatCentrewillverifytheabovesaidproofwithoriginals.

4. UploadingtheclientdetailstotheExchangesandDepositoryParticipants

5. OnreceiptofValidReport,accompanyingthecodesallocatedto clientsthesameis intimatedovertelephoneandWelcomeLetteralongwithzeroxcopyofKYCalongwith documentsreceivedfromtheclientissendtotheclient.Financialdetailsaretobe obtainedandupdatedthroughIncomeTaxreturnsandBalanceSheetorotherrelevant documents.Thisshallbedoneonaperiodicalbasis.

6. AnymodificationinClient'sdetailistobedoneonlyatthewrittenrequestfromclient along with required proof, if modification relates to Address, DP ID, and Bank Account,mobile,e-mailandetc.

7. AClientaccountistobeclosedonlyonwrittenrequestofClient.Ifrequestiseither fromclientorAuthorisedPersonthen30days'noticeistobesenttootherparty beforesuch closure.

8. Aseparateagreementistobesignedwithclient,whoeverwantstodoInternettrading.Different agreementistobesignedfordifferentPrincipalExchanges.

FinancialDocumentation: Allclientsarerequiredtosubmitupdatedfinancialdata,namely,their BalanceSheet,Salary Income Certificate. Incase of re-activation of UCC, the clients are also requiredtosubmitwrittenrequest.Clients,speciallyoperatinginF&OSegmentarecompulsorily requiredtosubmittheirlatestfinancialpositioneveryyearwithoutfail.

Maker&CheckerConcept: TheCompanyappointsdifferentpersonforcheckingCRF/data submitted by client and data entered in computer for uploading to master file & the Exchanges. Evenafteruploadingofdata,thedesignatedofficerchecksthedataenteredfromtheCRF.Allblank spacesintheCRFiscrossedbythedesignatedofficer,iffoundnotcrossedbytheclient.

Inactive/DormantAccountPolicy

IftheclienttradingcodeismarkedasInactive/Dormantfornon-executionofanytradesirrespective ofExchangeandSegmentinprecedingoneyear andwheretheclientisseekingforreactivation afteraperiodof1yearofbeingflaggedasinactive,theclientcodecanbeactivatedfortradingonly afterobtainingrequisiteapplicationandupdatedinformationrelatedtoKYCalongwiththeproper conductofIPV(In-PersonVerification)asmandatedbytheexchangesinsyncwiththeirrecently issuedcircularsinthemonthofDecember2020andclarificationissuedinthemonthofSeptember 2021.

However, in case a client has undertaken transaction through the Member,with respect to IPO/MutualFundsubscriptionandDPoperationsduringthisperiod,thesamecanbeconsidered andtherequirementforfreshdocumentation,duediligence,andIPVmaynotberequired.

Further, in thebelowmentioned conditions, as stipulated in SEBIcirculardated April 24, 2020, bearing reference number SEBI/HO/MIRSD/DOP/CIR/P/2020/73, the requirement for undertakinganIPVshallnotberequired:-

Wheretherespectiveclient'sKYCiscompletedusingtheAadhaarauthentication/verificationof UIDAI.

WhentheKYC formhasbeensubmittedonline,documentshavebeenprovidedthroughDigi lockeroranyothersourcewhichcouldbeverifiedonline.

Notwithstandinganythingcontainedabove,incaseaclientseeksre-activationbeforeaperiodof1 year of being flagged as inactive, BFSL shall,while reactivatingthe client, ensure that the basic detailsofsuchclientlikeAddress,PAN,Aadhaar,Mobilenumber,EmailID,Bank/DPaccountare updatedinitsrecordsaswellintheUCCrecordsoftheExchange.Incaseofanychanges, necessarydocumentsshallbecollectedandupdated(whereverrequired).

c.SENDING OF CONTRACT NOTES, DAILY MARGIN STATEMENT,STATEMENT OF ACCOUNTS

Processofissuanceof ContractNotes:

Acontract noteis the legal record of all transactions through stockbrokers on stock exchanges, and it includes all the trades executed on a particular day.The contract note formatis prescribed by the stock exchanges. A contract note should have the following details;

- Name,address, and SEBIRegistration numberof the stock broker.
- Nameofthepartners, proprietor,and theAuthorised Signatoryforthestock broker.
- Thedealing officedetailsand PANdetailsof thestock broker.
- TheUniqueClient CodeandPANof the Investor.
- TheContract notenumber, date ofissueofthecontract note,and thedate of settlement.
- Theorder numberand ordertimecorrespondingto thetrades.
- Thetradenumber and tradetime.
- Thequantityand detailsofsecurities bought/soldbythe client.
- Thetradeprice andthebrokerage(mentioned separately).
- StatutoryandRegulatorycharges asapplicable.

IssuanceofcombinedContractNotes&Margin Statement

Clientcanoptfor DigitalorPhysicalContractNote.

ForDigitally Opted clients:

- Contract Note & Margin Statement in PDF are sent via registered email to the clients within 24 hours of the execution of trades by Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member).
- Theattachmentfileispasswordprotectedforthe security ofthedocument.
- Log report of Contract note & Margin Statement is monitored on daily to ensure the delivery of the documents. For bounced contract notes & margin statement, if any, Physical Contract notes & Margin Statements are send to the registered address of the clients by Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member) through Post office service.

ContractNotes&Margin statementForPhysicalOptedClients:

PhysicalContractnote&Marginstatementaresendto theregisteredaddressoftheclients byVijayranga Enterprises & Intermediaries (P)Ltd(TradingMember)throughPostOfficeServicewithin24hoursof the execution of trades.

- Contract Note & Margin statement can also be downloaded by the registered clients from Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member) website: **veiblr.com** usingrespective client's user id and password.
- Old Contract Notes & Margin statement can also be downloaded by the clients from Vijayranga Enterprises & Intermediaries (P)Ltd(Trading Member) website: **veiblr.com** using respective client's user id and password.

ProcessofissuanceofSOA:

Weekly Statement of Accounts of Funds and weekly Statement of Accounts of Securities/Commodities for the period Monday to Saturday are sent via registered email to the clients within next four Trading days by Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member). Statements having nil transaction also are sent to all active clients who have done at least one trade for the past one year.

Log report of Weekly Statement is monitored on weekly basis to ensure the delivery of the documents. Forbounced statement, if any, Physical Statements aresend to the registered address of the clients by Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member) through Post office service.

D.REGARDINGFUNDS&SECURITIES

Clients'MoneyistobekeptinseparateaccountwithnomenclatureUSCNBasperSEBI/Exchange circulars.

1. EveryClients/APwillhavetomaintainbalanceagainstmarginspayablebyClients/AP.Margin canbedepositedinformofCASHandShares.
2. Collateral received as Margin pledge shares from the clients are re-pledged with clearing corporationorretainedwithVijayranga Enterprises & Intermediaries (P)LimitedandMarginbenefitwillbeprovidedtothe clientsaccordingly.
3. ASeparateDemat BeneficiaryAccount (StockBrokerProprietaryAccount)is tobeopened for keepingownsecuritiesofVijayranga Enterprises & Intermediaries (P).
4. Thepay-inobligationsofFunds/SecuritiesaretobemetuptoT+1inCashSegmentandin DerivativesSegmentandalsowithinprescribedtime.
5. ForPay-inobligationsofFunds,Cheques,NEFT/RTGSaretobereceivedfromclientsinthe name of Vijayranga Enterprises & Intermediaries (P)LimitedA/candcreditsaretobegivenonclearanceofchequesonly.

6. Pay-outoffundswillbegiventoclientsonformalrequestfromclients.Foranytransferof funds through Bank Transfer / RTGS, it is to be ensured by Department that funds are transferredonlyinthataccountofclient,whichislatestavailablewithusinourKYCForm.

7. SecuritiesPay-InProcess

After the introduction of Inter-Operability in clearing settlement obligations,Vijayranga Enterprises & Intermediaries (P) Ltd (Trading Member) has chosen NCL as designated Clearing House.

Securities Pay in Obligation of Clients are accepted only from mapped demat account of the respective clients to the NCL Pool account of the Trading Member through Block Mechanism. For this purpose, the Demat Accounts of the clients are mapped in back office of the Trading Member to ensuredelivery of shares is received from the respective client's mapped accounts only.

a) On T day, Securities Pay in Obligations of POA/DDPI executed clients are processed and blocked in clients demats accounts through Block Mechanism with Early Pay in to the Clearing Corporation. On Settlement Pay in day the blocked securities are debited and moved from clients demat accounts to Clearing Corporation's account by the Depositories.
b) NonPOA/DDPIclientsneedtodeliverPayinObligationofSecuritiestotheNCL Pool account of the Trading Member through Block Mechanism with Early Pay in, by themselves well within the prescribed Pay in time.
c) For any Shortfall, auction process/close out will be there according to Exchange Rules/Company Policy.

8. ForPay-outofSecurities

a) Securities received in pay-out, are transferred to the demat account of the respective clients directly from the Pool Account of the Trading Member with in one working day of the pay- out.

b) With regard to the unpaid securities (i.e., the securities that have not been paid for in full by the clients), such securities shall be transferred to respective client's demat account followed by creation of auto-pledge (i.e., without any specific instruction from the clients) with the reason "unpaid" in favour of a separate account titled "client unpaid securities pledgee account" (CUSPA)which shall be opened by TM/CM.

c) If the client fulfils its funds obligation within five trading days after the pay out, Trading Member / Clearing Member shall release the pledge so that the securities are available to the client as free balance.

d) In case of partial clearance of outstanding dues, securities pledged under CUSPAshallbepartially releasedto the client. However, if availability of single ISIN for the respective client in CUSPA, then such single security shall be released on the receipt of total dues, splitting of quantity and release shall not be processed.
e) If the client does not fulfils its funds obligation, TM/CM shall dispose of such unpaid securities in the market with in five trading days after the pay-out.
f) The unpaid securities shall be sold in the market with the Unique Client Code (UCC) of the respective client.Profit/Loss on the sale transaction of the unpaid securities, if any, shall be transferred to/adjusted from the respective client account.
g) TM/CM shall invoke the pledge only against the delivery obligation of the client.On invocation, the securities shall be blocked for early pay-in in the client's demat account with a trail being maintained in the TM/CM's client unpaid securities pledgee account.
h) In case, such pledge is neither invoked nor released within seven trading days after the pay-out, the pledge on securities shall be auto released and the securities shall be available to the client as free balance without encumbrance..

9. FundsPayOutProcess:

A. As per SEBI circular MIRSD/ SE /Cir-19/2009 dated December 3, 2009 and SEBI/HO/MRD/DP/CIR/P/2016/135datedDecember16,2016,thesettlement of funds and / or securities shall be done within 1 working day of the pay-out, unless client specifically authorizes the trading member in writing to maintain a running account.

B. Running account for securities has been discontinued and only running account of client's funds is applicable now. Vide SEBI circular no. CIR/HO/MIRSD/DOP/CIR/P/2019/75 dated June 20, 2019,

C. Settlement of running account of funds of the client shall be done by the Vijayranga Enterprises & Intermediaries (P)LimitedafterconsideringtheEndoftheday(EOD)obligationof funds as on the date of settlement across all the Exchanges on first Friday of the Quarter. If first Friday is a trading holiday, then such settlement shall happen on the previous trading day. (SEBI circular no. SEBI/HO/MIRSD/DOP/P/CIR/2022/101 dated July 27, 2022)

D. Forclients,whohaveoptedforMonthlysettlement,runningaccountshall be settled on first Friday of each month. If first Friday is a trading holiday

1. In case a client wishes to maintain a running account for its funds with the Vijayranga Enterprises & Intermediaries (P) Limited, the client has to authorize the VEI in writing to retain its funds. Such authorization should also contain:

- Mandate of the client as to whether the settlement of funds should be done on monthly / quarterly basis.

▪ A clause stating that the Client may revoke the authorization at any time (i.e.Without notice)

2. Running account authorization received through online secured access by way of client specific user id & password or through a registered email id of client is considered as authorization in writing.

InactiveClients Pay Out

a. Fortheclientshavingcreditbalance,whohavenotdoneanytransactionin the 30 calendar days since the last transaction, the credit balance will be returned to the client by Vijayranga Enterprises & Intermediaries (P) Limited, within next three working days irrespective of the date when the running account was previously settled.

b. Further, after settlement, if such client returns to the member with fresh funds and no trades are executed during this period, then BFSL may compute the 30 calendar days for the purpose of subsequent settlement from the day the member receives funds instead of the last transaction date.

c. However,BFSLshallsettlerunningaccountof clientonfirst Fridayofthe quarter or month as per as per the preference of the client irrespective of date of his/her last transaction or receipt of funds.

d. If the client has an open position in the derivatives segment, then the date of contract expiry or the date on which position is closed may be treated as last transaction date, for the purpose of computing 30 calendar days for returning the credit balance to such clients. However, VEI shall ensure settlement of running account of funds on first Friday of the Month or Quarter as per the preference of the client.

e. If the client executes a transaction on the Exchange on or before the date on which VEI is scheduled (within three working days) to return the credit balance, in that case, the VEI may retain the funds as clarified in Point 5 and settle the balance amount to client.

Retentionof Funds

In case of client having any outstanding trade position on first Friday of the Month / Quarter on which settlement of running account of funds is scheduled, Vijayranga Enterprises & Intermediaries (P) Limited will retain funds calculated in the manner specified below:

i. Entirepay-inobligationoffundsoutstandingattheendofdayondateof settlement, across all segments.

ii. Membermayretain50%ofendoftheday(EOD)marginrequirementascash margin, excluding the margin on consolidated crystallized obligation/ MTM.

iii. Apart from 50% cash margin mentioned in point ii above, member may alsoretain 225% of EOD margin (which includes additional 125% margin) reduced by 50% cash margin and the value of securities (after applying appropriate haircut) accepted as collateral from the clients by way of 'margin pledge' created in the Depository system for the purpose of margin and value of commodities (after applying appropriate haircut). The margin liability shall include the end of the day margin requirement in all the segments across exchanges excluding the margin on consolidated crystallized obligation/ MTM. The margin liability may also include the margin collected by the Member from their clients as per the risk management policy and informed to the clients.

10. NofundingistobegiventoClients/AuthorisedPerson.

E. CONTROLOVERBRANCHESANDTERMINALS

1. EveryAuthorisedPersonOfficewillbetreated asBranchforControlpurposes.
2. Newterminalwillbeallottedonwrittenrequestof/AuthorisedPerson
3. BeforeallottingterminaI,documentssuchasNOC,certification,rentagreement, ownershipproofandlocationistobecheckedbyMembershipDepartment.
4. Location of terminals / trading terminals is granted only at Trading Members' RegisteredOffice,Branch Office and their Registered Authorised Person Offices.
5. Allotment details of terminals are to be uploaded with respective Stock Exchanges.
6. RegularInspectionsandsurprisechecksaretomadetocontrolunauthorizeduse of terminals.
7. Details of Terminals, Broker, Authorised Person, SEBI Registration Number, PrincipalOfficerdetails,ComplianceOfficerdetailsetc.aretobeaffixedatthe placeofoperationofterminals.
8. Details ofcertification, which isgoingtobeexpired should bepreparedin advance, preferably60 days and should be informed to concerned Authorised Person to submitnewcertificationelseterminalsaretobede-activated.
9. 30% of Authorised Persons should be inspected every year and this inspection is to bedonebyrotationtocovereachandeveryAuthorisedPersonwithinprescribed time.

10. Trading Limits are given and monitored according to policies of Risk Management Committee&BoardoftheCompanyandrulesandregulationsofExchanges/SEBI.

F. PMLA

1. Principal Officer of the Company under PMLA is to be appointed and informationtobesenttoFIU.
2. Written Policy under PMLA should be made to prevent Money Laundering activities.
3. Sufficientverifieddocumentationandinformationistobeobtainedsothatno fictitious,benamiaccountisopened.
4. Volume of trading done by the Client should be checked and matched with financial detailsavailablewiththeCompany.Thisshouldbedoneperiodically.
5. Ifthereisanysuspicioustransaction,theinformationofsaidtransactionistobesentto FIUthroughsuspicious Transaction Report (STR).
6. AsperPMLA,2002sub-brokers/AuthorisedPersonshouldkeepawatchonthe tradingactivitiesof'ClientofSpecialCategory',whichincludes,non-residentclients andcompanieshavingclosefamilyshareholdingsorbeneficialownerships.

G. <u>OTHERS</u>

1. PowerofAttorneyistobeexecutedonNonJudicialStampPaperofrequisitevalue.
2. POA/DDPIistobelimitedtooperatetheBeneficiaryOwnerAccountforlimited purposeasspecifiedinSEBIcircularno.SEBI/HO/MIRSD/DOP/CIR/P/2020/158 dated August 27, 2020 (“PoA Guidelines, 2020”) and vide SEBI Circular SEBI/HO/MIRSD/DoP/P/CIR/2022/44datedApril04,2022.
3. PowergiveninPOAcanberevokedatanytimewithoutpriornoticebutunder intimationtoVijayranga Enterprises & Intermediaries (P)Limited.
4. ANewPowerofAttorneyistobeobtainedif thereisanychangeinconstitutionof account.

AUTHORISEDPERSONPOLICY

AUTHORISEDPERSONPOLICY(REGISTRATION,CANCELLATION & INSPECTION)

REGISTRAION

Once an Individual/Corporate is willing to become an AP. The AP has to provide his all the relevant documents of his identity and address with the education proof. The Prescribed Educational Qualification by Exchanges.

Vijayranga Enterprises & Intermediaries (P) Limited will conduct due diligence by means of In – person Verification, site visits, validating the PAN and conduct background check ensuring the applicant is not part of SEBI & Exchange debarred list before on boarding.

Then AP has to enter into an agreement as formalized by the exchange and also with the Vijayranga Enterprises & Intermediaries (P) Limited.

Once the documents are received and verified by the Membership Department the same will be uploaded to the exchange portal for the process of Registration as AP.

Oncethe APgets registered,the registrationdetailswillbeinformedto AP through the Email.

After the AP is registered with Exchange the permission of Trade will be processed by Membership Department.

TheMembershipDepartmenthastoinitiateTrade permissiononreceiptof:

a. ReceiptofMinimumCapitalAdequacy(SecurityDeposit)
b. SignedBrokerageSheet
c. UserId formforTerminalActivation
d. NISMCertificateincase ofF&OActivation

CANCELLATION

IfanAPisdesiroustocancelhisAPregistration,hehastogivewrittenrequestletterfor cancellation.

Once the request is received, his trading terminal will be deactivated after sending notice to his clients.

After 30 days his terminal; will be de-activated and his cancellation request will be submitted to exchange for further process.

After cancellation is approved by the exchanges the Security deposit amount taken from the AP at the time of registration will be with Locked In for a period of six months from date of cancellation for meeting any kinds of client claims and grievances.

DE-ACTIVATION

Vijayranga Enterprises & Intermediaries (P) Limited will de-activate the trading terminals of Authorised Person where no trades have been placed in last six months or have been inactive

INSPECTION

Vijayranga Enterprises & Intermediaries (P) Limited will exercise adequate control and due diligence over the activities of the Authorised Person by conducting surprise and periodic Inspection.

Vijayranga Enterprises & Intermediaries (P) Limited will be conducting regular inspection based on the Volume/turnover of the registered Authorised Person as per the below criteria

RevisedCriteriabasedon volumes/ turnover	PeriodofInspection
Top50%ofRegisteredAPs	Oncea Year
SubsequentTop30%ofRegisteredAPs	Oncein18 months
Remaining20%ofRegisteredAPs	Oncein2 years

Vijayranga Enterprises & Intermediaries (P) Limited for effectiveness of the supervision and inspection of Authorised Person will adhere following guidelines as mentioned by the Exchanges:

i. Whetherallclientsare registered directlywiththeTradingMemberonly.
ii. Adequatesystems, including voice recording, have been put in place, with a view to ensure recording of order placement from clients. Trading Members must ensure that APs who do not have trading terminals assigned to them, cannot place trades on behalf of the Trading Member's clients.
iii. There is no movement of Funds and securities between the client and AP for settlement of trades on the Exchange. Demat statement and bank accounts of the AP to be examined to verify such instances.
iv. Therearenocash dealingsdoneby AP.
v. Documents like contract notes, statement of funds, daily margin statement are not generated and issued by the AP. However, AP may provide administrative assistance in procurement of documents from the Trading Member, after maintaining proper records of the same.
vi. AllAP terminalsareasper theinformation reportedto theExchange.
vii. Tradingterminalsareoperatedby approvedandcertifiedusers.
viii. Notice board of the Trading Member containing all details/information prescribed from time to time, are displayed at the AP/s location.

ix. SEBI registration certificate of the Trading Member and registration letter issued by the Exchange is displayed at the location.

x. As required by SEBI circular CIR/MIRSD/3/2014 dated August 28, 2014,information about the grievance redressal mechanism available to investors is prominently displayed at the location.

xi. TheAuthorisedPersonisnotinvolvedinanyfund-basedactivities/collectingdeposits from investors/unauthorized trading/chit funds or any other such schemes.

xii. The AP has not dealt with any other Trading Member/AP on behalf of its clients/self on the same Stock Exchange.

xiii. APhasnotdealt withanyunregisteredintermediary onbehalfofits clients/self.

xiv. TheAP is not involved in accepting deposits from the public and giving assured returns to their clients.

xv. Advertisements for soliciting business are not issued by the APs in newspapers/pamphlets /journals/magazines etc., without seeking appropriate approvals from the Exchange, through the Trading Member.

xvi. Complaints received by and against the APs are handled appropriately and proper records are maintained.

xvii. Trading activities/Turnover of APs are monitored, and necessary actions/investigations are undertaken on a timely basis. Trading Member shall de-activate all trading terminals extended to AP which are inactive for more than 6 months and update the Exchange records. Appropriate due diligence to be undertaken in case of re-activation of such terminals.

xviii. The AP has the necessary infrastructure like adequate office space, equipment, and manpower to effectively discharge the activities on behalf of the Trading Member.

xix. Proper segregation and demarcation are maintained at AP office for any permissible activity other than the broking business.

xx. Branch/AP records/data are properly maintained with confidentiality in a secure manner including sufficient backup.

xxi. IncaseofchangeshiftingoflocationofAP/Branch,thefollowingisensured:

a) AllclientsmappedtotheAP/BrancharenotifiedatleastthirtydaysbeforethechangeNotice Board and applicable SEBI registration certificates are immediately put up at the new location.

c) ThenewlocationshallbedulyreportedtotheExchangeandtheoldlocation should be deactivated. New terminal details shall also be uploaded to the Exchange. Vijayranga Enterprises & Intermediaries (P)Limitedwillretainthereportofinspection/visitconductedfora period of five years.

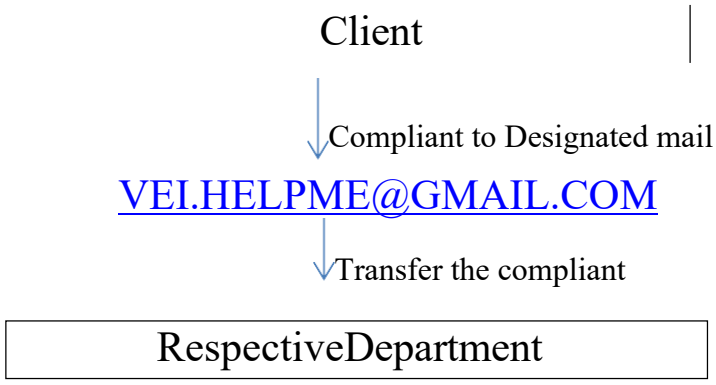
INVESTORSGRIEVANCESPOLICY

INVESTORGRIEVANCEREDRESSALMECHANISMPOLICY

TheInvestor GrievanceishandledattheRegisteredHead Office,Bangalore.

1. Thecompanyhasadesignatedemail IDvei.helpmeforreceivingcomplainsby itsclients.TheemailIdhasbeendisclosedintheKYCKitsenttoallclientsatthetime of registration as well as is mentioned on the contract note.
2. Onreceivingthecomplain,theDesignatedofficerhastoforwardthecomplianttothe respective department for speedy redressal.
3. Oncethe compliant isredressedthedesignatedofficerwillwritepersonally totheclient.
4. If the compliance officer deserves the attention of the higher management or if the complianceofficerisunabletodisposeofcomplaintothesatisfactionoftheclientorthe exchange or the SEBI, the designated directors are informed of the situation by the compliance officer and all documents are placed before them within seven days of the receipt of the complain.
5. Thedesignateddirector'sreviewthependingcomplainseverysevendaysalongwith matters needed their attention.

FlowChart



Note:Oncethegrievancesarere

dresseditisinformedtotheclients.

OUTSOURCINGPOLICY

OUTSOURCINGPOLICY

INTRODUCTION

1. Outsourcing means the use of one or more than one "Third Party", either within or outside the group, by a Registered Intermediary to perform the activities associated with services which the intermediary offers. A third party may be used to perform one or more activities or one or more third parties may be used to perform different activities associated with the intermediation service. Such use may be for a specified period or on a continuing basis. However, there are various risks associated with outsourcing which may be identified as operational risk, reputational risk, legal risk, country risk, strategic risk, exit-strategy risk, counter party risk, concentration and systemic risk.

2. In order to address the concerns arising from the outsourcing of activities by intermediaries based on the principles advocated by the International Organization of Securities Commission (IOSCO) and the experience of Indian markets, SEBI had prepared guidelines on outsourcing of activities related to services offered by intermediaries.

3. In pursuance of SEBI Circular No.CIR/MIRSD/24/2011 dated December 15, 2011, a policy on Outsourcing of Activities by Intermediaries needs to be in place to ensure high standards of continuing services and exercise due diligence and proper care in its operations.

SCOPE

1. This policy is to be applied by the Board of Directors, Senior Management and Employees of, the Company, at the time of outsourcing activities.

2. Thekey purposes of thepolicy are as follows:

a) Toestablishacomprehensiveriskmanagementprogrammetoaddresstheoutsourced activities and the relationship with Service Provider

b) ToconductduediligenceoftheServiceProvidertoascertainthecredibilityand capability of the Service Provider.

c) Tomaintainconfidentialityof theinformationthatis outsourced.

d) Toensurecompliance withthelawsandregulationsin forcefromtimeto time.

e) Toprotect theCompany reputation.

f) Toconductoutsourcingofactivitiesinaccordancewiththis policy.

g) Toidentify thesupervisorsand fix theirresponsibilities.

ACTIVITIESNOTTOBE OUTSOURCED

1. Companyshallnotoutsourceitscorebusinessactivitiesandcompliancefunctions. Core Business activities such as:

• Executionofordersand monitoringoftradingactivitiesof

• Dematerializationofsecuritiesincaseofdepositoryparticipants;

• InvestmentrelatedactivitiesincaseofMutualFundsandPortfolioManagers.

• Regarding KnowYourClient (KYC) requirements, weshall comply with the provisions of SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011 and Guidelines issued there under from time to time.

POLICY FOR VOLUNTARY FREEZING OF ONLINE ACCESS OF CLIENT'STRADING ACCOUNT

Policyforvoluntaryfreezingofclient'sonline access

1. Background:

SEBI vide it's circular SEBI/HO/MIRSD/POD-1/P/CIR/2024/4 dated January 12, 2024 and Exchanges vide their circulars dated April 08, 2024 mandated trading members to provide the facility of voluntary freezing/blocking the online access of the trading account to their clients on account of suspicious activities.

The said circular also requires the trading members to frame a policy in line with the frameworkspecified by theExchanges, which shall bethepartofthetrading member's Risk Management Policy. The trading members shall disclose the said policy on their website. The said policy shall also form a part of the account opening kit for all new clients onboarded with effect from July 01, 2024.

2. Scope: This policy shall be applicable when clients requires to freeze / block online access to their trading account and subsequently desires to unfreeze the same.

3. Frameworkforvoluntaryfreezingofonlineaccessofclient'stradingaccount–

a. Requestforfreezing

i. Client may request for voluntary freezing / blocking the online access to their trading account through any one of the following modes that shall be made –

BysendinganEmailfromregisterede-mailIDrequestingforfreezing/blockingto veiblr@gmail.com

BySubmittingtheformatourwebsite veiblr.com inunder theheadAccount freeze.

ii. Theclient shallsubmit arequest for freeze.

iii. On receipt of such request, the online access of the client's trading account shall be freezed/blocked.

iv. Post freezing/blocking the client's trading account, a communication shall be sent on the registered mobile number and registered e-mail ID of the client, stating that the onlineaccess to the trading account has been frozen/blocked.

v. Details of open positions (if any) shall also be communicated to the client along with contract expiry information within such time as prescribed by regulators. This will eliminate the risk of unwanted delivery settlement.–

a. Request forUn-freezing

vi. Client may request for unfreezing / unblocking the online access to their trading account by sending email at VEI.HELPME@GMAIL.COM from client's registered email.

b. Importantpoints

vii. All logs of freeze and unfreeze request and communications sent shall be maintained for audit trail.

viii. Freezing/blocking is only for the online access to the client's trading account, and there shall be no restrictions on the Risk Management activities of Vijayranga Enterprises & Intermediaries (P) Limited.

ix. The request for freezing/ blocking does not constitute request for marking client Unique Client Code (UCC) as inactive in the Exchange records.

x. The freeze, unfreeze, issue of communication shall be within the timelines specified bySEBI / Exchanges in this regard.

4. PolicyReview: ThesaidpolicyshallbeapartofVijayranga Enterprises & Intermediaries (P)LimitedRiskManagement Policy and shall be reviewed along with the said policy on a half yearly basis.

Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing ofTerrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention ofMoney Laundering Act, 2002 and Rules framed there under.

1. The Prevention of Money Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules1), as amended from time totime and notified by the Government of India, mandate every reporting entity [which includes intermediaries registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBIAct) and stock exchanges], to adhere to client account opening procedures, maintain records and report such transactions as prescribed therein to the relevant authorities. The PML Rules, inter alia, empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and the form in which such information is to be maintained.Italsomandatesthereportingentitiesto evolveaninternalmechanismhavingregard to any guidelines issued by regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by the regulator.

2. The enclosed guidelines stipulate the essential principles for combating Money Laundering (ML) and Terrorist Financing (TF) and provide detailed procedures and obligations to be followed and complied with by all the registered intermediaries.

3. These guidelines shall also apply to the branches of the Stock Exchanges, registered intermediaries, and their subsidiaries situated abroad, especially, in countries which do not apply or insufficiently apply the recommendations made by the Financial Action Task Force (FATF),to the extent local laws and regulations permit. When the local applicable laws and regulations prohibit implementation of these requirements, the same shall be brought to the notice of SEBI.

4. SEBI has from time to time issued circulars/directives with regard to Know Your Client (KYC), Client Due Diligence (CDD), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) specifying the minimum requirements. It is emphasized that the registered intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address the concerns of money laundering and suspicious transactions undertaken by clients.5. On and from the issue of this Circular, the earlier circulars issued by SEBI on the subject of Anti-Money Laundering and Combating the Financing of Terrorism, listedoutintheAppendix,shallstandrescinded. Notwithstandingsuchrescission, anythingdone or any action taken or purported to have been done or taken under the circulars sp edified in Appendix, shall be deemed to have been done or take under the corresponding provisions of this Master Circular.

6. This Master Circular shall supersede the previous Master Circular reference no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 and is available at www.sebi.gov.in under the link "Legal Master Circulars".

1. The Directives as outlined below provide a general background and summary of the main provisions of the applicable anti-money laundering and anti-terrorist financing legislations in India. They also provide guidance on the practical implications of the Prevention of Money Laundering Act, 2002 (**PMLA**). The Directives also set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities.

2. These Directives are intended for use primarily by intermediaries registered under Section 12 of the Securities and Exchange Board of India Act, 1992 **(SEBI Act),** Stock Exchanges, Depositories and other recognized entities under the SEBI Act and Regulations and rules thereunder**.** While it is recognized that a "one-size-fits-all" approach may not be appropriate for the securities industry in India, each registered intermediary shall consider the specific nature of its business, organizational structure, type of clients and transactions, etc. when implementingthesuggestedmeasuresandprocedurestoensurethattheyareeffectivelyapplied.Theover riding principle is that they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

Background

3. As per the provisions of PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time and notified by the Government of India, every reporting entity (which includes intermediaries registered under section 12 of the SEBI Act, i.e. a stockbroker, share transfer agent, banker to an issue, trustee toa trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the SEBI Act and stock exchanges), shall have to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

The PML Rules empower SEBI to specify the information required to be maintained by the intermediaries and the procedure, manner and form in which it is to be maintained. It also mandates the reporting entities to evolve an internal mechanism having regard to any guidelines issued by the regulator for detecting the transactions specified in the PML Rules and for furnishing information thereof, in such form as may be directed by SEBI.

4. The PMLA inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as provided in Section 12A read with Section 24 of the SEBI Act will be treated as a scheduled offence under schedule B of the PMLA.

PoliciesandProcedurestoCombatMoneyLaunderingandTerroristFinancing

Essential Principles:

5. These Directives have taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act.The detailed directives have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

6. In case there is a variance in Client Due Diligence (CDD)/ Anti Money Laundering (AML) standards specified by SEBI and the regulators of the host country, branches/overseas subsidiaries of registered intermediaries are required to adopt the more stringent requirements of the two.

7. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, financial groups shall be required to apply appropriate additional measures to manage theML/TF risks and inform SEBI.

Obligationtoestablishpoliciesandprocedures

8. Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all registered intermediaries ensure the fulfilment of the aforementioned obligations.

9. The term “group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of Rule 2 of the PML Rules as amended from time to time. Groups shall implement group-wide policies for the purpose of discharging obligations under Chapter IV of the PMLA.

10. Financial groups shall be required to implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group as under:

a. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

b. the provision, at group level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This shall include information and analysis of transactions or activities whichappearunusual(ifsuchanalysiswasdone);similarprovisionsforreceiptofsuch

information by branches and subsidiaries from these group level functions when relevant and appropriate to risk management; and

c. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

11. To be in compliance with these obligations, the senior management of a registered intermediary shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The registered intermediaries shall:

i. issueastatementofpoliciesandproceduresand implement,onagroup basiswhereapplicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;

ii. ensurethatthe contentoftheseDirectivesareunderstood byallstaffmembers;

iii. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies andprocedures;

iv. adoptclientacceptancepoliciesandprocedureswhicharesensitivetothe risk of ML and TF;

v. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

vi. haveasysteminplaceforidentifying,monitoringandreportingsuspectedMLorTFtransactions to the law enforcement authorities; and

vii. developstaffmembers'awarenessandvigilancetoguardagainstMLandTF.

12. Policiesandprocedurestocombat MLandTFshall cover:

i. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;

ii. Client acceptance policy and client due diligence measures, including requirements for proper identification.

iii. Maintenanceofrecords.

iv. Compliancewithrelevantstatutoryandregulatoryrequirements.

v. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information.

vi. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, 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; and,

vii. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

WrittenAnti MoneyLaundering Procedures

13. Each registered intermediary shall adopt written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia,the following four specific parameters which are related to the overall 'Client Due Diligence Process':

i. Policyforacceptanceof clients;
ii. Procedureforidentifyingtheclients;
iii. Risk Management;
iv. Monitoring of Transactions.

ClientDueDiligence(CDD)

14. Client Due Diligence means due diligence carried out on a client referred to in clause (ha) of sub-section (1) of section 2 of the PMLA using reliable and independent sources ofidentification.

15. The CDD shall haveregard to the money laundering and terrorist financing risks and the size of the business and shall include policies, controls and procedures,approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the registered intermediary or through national risk assessment.

16. TheCDDmeasures comprise thefollowing:

i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using reliable and independent client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement;

ii. Identify the clients, verify their identity using reliable and independent sources of identification,obtaininformationonthepurposeandintended natureofthebusinessrelationship, where applicable;

iii. Verifytheclient'sidentityusingreliable,independentsourcedocuments, dataorinformation. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorizedandverifytheidentityofthatpersonProvidedthatincaseofaTrust,thereporting

entity shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

iv. Identifying beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted. The beneficial owner shall be determined as undera) **where the client is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation:-For thepurposeof this sub-clause:-

i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company.

ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders' agreements or voting agreements.

b) **where the client is a partnership firm**, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation:-Forthepurposeofthisclause:-"Control"shallincludetherighttocontrolthe management or policy decision.

c) **where the client is an unincorporated association or body of individuals,** the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent of the property or capital or profits of such association or body of individuals.

d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

e) **Where the client is a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust, settlor, protector and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government or it is a subsidiary

of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

g) **Applicabilityforforeigninvestors**:Registeredintermediaries dealing withforeigninvestors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022, and amendments thereto, if any, for the purpose of identification of beneficial ownershipof the client.

h) The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other registered intermediaries, by their Board of Directors.

v. Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to

vi. Understandthenatureofbusiness, ownershipand controlstructureoftheclient;

vii. Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

viii. Registered intermediaries shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data.

ix. Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due Diligence is kept up-to-date and relevant, particularly for high-risk clients.

x. Everyregisteredintermediaryshallregisterthedetailsofaclient,incase ofclientbeinganon- profit organization, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

xi. Where registered intermediary is suspicious that transactions relate to money laundering or terroristfinancing,andreasonablybelievesthatperformingtheCDDprocesswilltip-offthe

client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND.

17. No transaction or account-based relationship shall be undertaken without following the CDD procedure.

Policy foracceptanceofclients

18. All registered intermediaries shall develop client acceptancepolicies and procedures that aim to identify the types of clients that are likely to pose a higher-than-average risk of ML or TF. By establishing such policies and procedures, they will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. Inanutshell,thefollowingsafeguards aretobe followedwhile acceptingtheclients:

i. No registered intermediary shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

iii. The registered intermediaries shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

a) Non- residentclients.
b) Highnet-worth clients.
c) Trust,Charities,Non-GovernmentalOrganizations(NGOs)andorganizationsreceivingdonations.
d) Companieshavingclosefamilyshareholdingsorbeneficialownership.
e) Politically Exposed Persons" (PEPs). PEP shall have the same meaning as given in clause (db.) of sub-rule (1) of rule 2 of the PML Rules. The additional norms applicable to PEP as contained in the subsequent paragraph 20 of the master circular shall also be applied to the accounts of the family members or close relatives / associates of PEPS.

f) Clients in high-risk countries. While dealing with clients from or situated in high-risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action againstmoneylaunderingorterrorfinancingissuspected,registeredintermediariesapartfrombeing

guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatfgafi. org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However,thisshallnotprecluderegisterintermediariesfromenteringintolegitimatetransactions with clients from or situated in such high-risk countries and geographic areas or delivery of servicesthroughsuchhigh-riskcountriesorgeographicareas.Theintermediaryshallspecifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

g) Non face to face clients - Non face to face clients means clients who open accounts without visiting the branches/offices of the registered intermediaries or meeting the officials of the registered intermediaries. Video based customer identification process is treated as face-to-face onboarding of clients.

h) Clientswithdubiousreputationasperpublicinformationavailable etc.

The above-mentioned list is only illustrative, and the intermediary shall exerciseindependentjudgmenttoascertainwhether anyothersetofclientsshallbe classifiedasCSC or not.

iv. Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

v Ensure that an account is not opened where the intermediary is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non - genuine, or thereis perceived non - co-operation of the client in providing full and complete information. The registered intermediary shall not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whetherto freeze or close the account. The registered intermediary shall be cautious to ensure that it does not return securities or money that may be from suspicious trades. However, the registered intermediaryshallconsulttherelevantauthorities indeterminingwhatactionitshalltakewhenit suspects suspicious trading.

vi. The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall be operated, transaction limits for the operation, additional authority required for transactions exceeding as specified quantity/value and other appropriate details. Further the rights and responsibilitiesof both thepeoplei.e.the agent-clientregistered withthe intermediary, aswellas

the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

vii. Necessary checks and balance to be put into place before opening an account so as to 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.

viii. TheCDDprocessshallnecessarilyberevisitedwhenthere aresuspicionsof ML/TF.

Clientidentificationprocedure

19. The KYC policy shall clearly spell out the client identification procedure (CIP) to be carried outatdifferentstagesi.e.whileestablishingtheintermediary –clientrelationship,whilecarrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

20. Registered intermediaries shall be in compliance with the following requirements while putting in place a CIP**:**

i. All registered intermediaries shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.

ii. All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

iii. Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

iv. The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information tosatisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance ofa copy.

vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.

21. SEBI has specified the minimum requirements relating to KYC for certain classes of registered intermediaries fromtimetotime.Takingintoaccountthe basic principlesenshrinedin the KYC norms which have already been specified or which may be specified by SEBI fromtime to time, all registered intermediaries shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices.

22. Further, the intermediary shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing.

23. Every intermediary shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of informationand verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to registered intermediaries (brokers, depository participants, AMCsetc.)fromobtainingtheminimum information/documentsfromclientsasstipulatedinthe PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly implemented by all registered intermediaries and non-compliance shall attract appropriate sanctions.

RelianceonthirdpartyforcarryingoutClientDueDiligence (CDD)

24. Registeredintermediariesmay relyona third partyfor thepurposeof-

i. identificationandverificationoftheidentityofaclientand

ii. Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place

forcompliancewithCDDandrecord-keepingrequirementsinlinewiththeobligations under the PML Act.

25. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. In terms of Rule 9(2) of PML Rules:

i. The registered intermediary shall immediately obtain necessary information of such client due diligence carried out by the third party;

ii. The registered intermediary shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

iii. The registered intermediary shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

iv. Thethird partyis notbased ina countryor jurisdictionassessed ashighrisk;

v. The registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

Risk Management

Risk-basedApproach

26. Registered intermediaries shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard.

Further,theregisteredintermediariesshallmonitortheimplementationofthecontrolsandenhance them if necessary.

27. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the Riskbased approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

28. Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

Risk Assessment

29. Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

30. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

31. The Stock Exchanges and registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:

a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

b. Adoption of a risk based approach to manage and mitigate the risks.

32. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

Monitoring of Transactions

33. Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that it can identify deviations in transactions activities.

34. The intermediary shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits.

The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made

Available to auditors and also to SEBI/stock exchanges/FIU-IND/other relevant Authorities, during audit, inspection or as and when required.

35. The registered intermediaries shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client.

36. The intermediary shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the higher authorities within the intermediary.

37. Further, the compliance cell of the intermediary shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

Suspicious Transaction Monitoring and Reporting

38. Registered Intermediaries shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, registered intermediaries shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

39. A list of circumstances which may be in the nature of suspicious transactions is given below. This 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:

i Clients whose identity verification seems difficult or clients that appear not to cooperate.

ii Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;

iii Clients based in high risk jurisdictions;

iv Substantial increases in business without apparent cause;

v Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

vi Attempted transfer of investment proceeds to apparently unrelated third parties;

vii Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

40. Any suspicious transaction shall be immediately notified to the **Designated/Principal Officer** within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

41. It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that registered intermediaries shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

42. Paragraph 18 (iii) (f) of this Circular categorizes clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. Registered intermediaries are directed that such clients shall also be subject to appropriate counter measures. These measures may include ab further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

Record Management

Information to be maintained

43. Registered Intermediaries are required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

i. The nature of the transactions;

ii. The amount of the transaction and the currency in which itis denominated;

iii. The date on which the transaction was conducted; and

iv. The parties to the transaction.

Record Keeping

44. Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

45. Registered Intermediaries shall 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 for prosecution of criminal behaviour.

46. In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail:

i. The beneficial owner of the account;
ii. The volume of the funds flowing through the account; and
iii. For selected transactions:
a. The origin of the funds
b. The form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
c. The identity of the person undertaking the transaction;
d. The destination of the funds;
e. The form of instruction and authority.

47. Registered Intermediaries shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

48. More specifically, all the registered intermediaries shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

ii. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency; It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from ‘transactions integrally connected’, ‘transactions remotely connected or related’ shall also be considered.

iii. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

iv. all suspicious transactions 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 maintained by the registered intermediary.

49. Where the registered entity does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which the registered intermediary shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules.

Retention of Records

50. Registered intermediaries shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and intermediary.

51. As stated in paragraph 19 and 20, registered intermediaries are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

52. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

53. Registered Intermediaries shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the intermediary.

Procedure for freezing of funds, financial assets or economic resources or related services

54. The Stock exchanges and the registered intermediaries shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments there to, they

do not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

55. In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08,2021(Annexure2). Corrigendums dated March15,2023and April 22, 2024 have also been issued in this regard (Annexure 3) and (Annexure 4). The list of Nodal Officers for UAPA is available on the website of MHA.

Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries

56. The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.

57. IntermsofSection12AoftheWMDAct,the CentralGovernmentisempoweredas under:

"(2) For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Actfor the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

(a) Freeze,seize orattach fundsor otherfinancialassetsor economicresources—

(i) ownedorcontrolled, whollyorjointly, directlyorindirectly, bysuchperson; or

(ii) heldbyor onbehalfof, orat thedirectionof, suchperson; or

(iii) derivedorgeneratedfromthefundsorotherassetsownedorcontrolled,directlyor indirectly, by such person;

(b) prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Actfor the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

58. The stock exchanges and registered intermediaries are directed to comply with the procedure laid down in the said Order.

59. The stock exchanges and registered intermediaries shall:

(i) Maintain the list of individuals/entities ("**Designated List"**) and update it, without delay, in terms of paragraph 2.1 of the Order;

(ii) verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), without delay.

The details of the CNO areas under:

The Director

FIU-INDIA

Tel.No.:011-23314458,011-23314459 (FAX)

Email: dir@fiuindia.gov.in

(iii) run a check, on the given parameters, at the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc. In case, the clients' particulars match with the particulars of Designated List, stock exchanges and registered intermediaries shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., held on their books to the CNO, without delay;

(iv) send a copy of the communication, mentioned in paragraphs 59(ii) and 59(iii) above, without delay, to the Nodal Officer of SEBI. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the Nodal Officer of SEBI Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051;

(v) prevent such individual/entity from conducting financial transactions, under intimation to the CNO, without delay, in case there are reasons to believe beyond doubt that funds or assets held by a client would fall under the purview of Section 12A (2)(a) or Section 12A(2)(b) of the WMD Act;

(vi) file a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts, covered under paragraphs 59(ii) and (iii) above, carried through or attempted through.

60. Upon the receipt of the information above, the CNO would cause a verification to be conducted by the appropriate authorities to ensure that the individuals/entities identified are the ones in the Designated List and the funds, financial assets or economic resources or related services, reported are in respect of the designated individuals/entities. In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under section 12A would be issued by the CNO and be conveyed to the concerned reporting entity so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/entities.

61. Reporting entities shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of Designated Individuals / Entities

62. The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. The registered intermediaries shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

63. All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

64. An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at https://press.un.org/en/content/press-release. The details of the lists are as under:

i. The “ISIL (Da’esh) & Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: https://www.un.org/securitycouncil/sanctions/1267/press-releases ;

ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

65. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all

existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

66. The Stock Exchanges and the registered intermediaries shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

67. The Stock Exchanges and the registered intermediaries shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

68. The Stock exchanges and the registered intermediaries shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

69. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

70. The Stock exchanges and the registered intermediaries shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay.

The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, “G” Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

Jurisdictions that do not or insufficiently apply the FATF Recommendations

71. FATF Secretariat after conclusion of each of it’s plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by the registered intermediaries.

72. The registered intermediaries shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

Reporting to Financial Intelligence Unit-India

73. In terms of the PML Rules, registered intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,

Financial Intelligence Unit- India

6th Floor, Tower-2, Jeevan Bharati Building,

Connaught Place, NewDelhi-110001, INDIA

Telephone: 91-11-23314429, 23314459

91-11-23319793

(Helpdesk) Email: helpdesk@fiuindia.gov.in (For FIN net

and general queries)

ctrcell@fiuindia.gov.in

(For Reporting Entity/Principal Officer registration related queries)

complaints@fiuindia.gov.in

Website: http://fiuindia.gov.in

74. Registered intermediaries shall carefully go through all the reporting requirements (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Brochures on FIU_p.pdf) and formats that are available on the website of FIU – IND under the Section Home - FINNET 2.0 – User Manuals and Guides -Reporting Format (https://www.sebi.gov.in/sebi_data/commondocs/jun-2024/Reporting_Format_p.pdf). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIUIND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, registered intermediaries shall adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month;

ii. The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 of the PML Rules. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion;

iii. The Non Profit Organization Transaction Reports (NTRs) for each shall be submitted to FIU-IND by 15th of the succeeding month;

iv. The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

v. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND;

vi. No NIL reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported;

vii. "Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-taxAct,1961 (43of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013);

viii. Every registered intermediary, its Directors, officers and all employees shall ensure that the fact of maintenance referred to in Rule 3 of PML Rules and furnishing of information to the Director is kept confidential. Provided that nothing in this rule shall inhibit sharing of information under Rule 3A of PML Rules of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

75. Registered Intermediaries shall not put any restrictions on operations in the accounts where an STR has been made. Registered intermediaries and their 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. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level. It is clarified that the registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

It is further clarified that "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence. Confidentiality requirement does not inhibit information sharing among entities in the group.

Designation of officers for ensuring compliance with provisions of PMLA

76. **Appointment of a Principal Officer:** To ensure that the registered intermediaries properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would 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 and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary; Provided that such officer shall be an officer at the management level.

77. **Appointment of a Designated Director**: In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

"Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,

b) the managing partner if there porting entity is a partnership firm,

c) the proprietor if there porting entity is a proprietorship firm,

d) the managing trustee if there porting entity is a trust,

e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above".

78. In terms of Section 13(2) of the PMLA, the Director, FIU –IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

79. Registered intermediaries shall communicate the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU – IND.

Hiring and Training of Employees and Investor Education

80. Hiring of Employees: The registered intermediaries shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

81. Training of Employees: The registered intermediaries shall have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

82. Investor Education: Implementation of AML/CFT measures requires registered intermediaries to demand certain information from investors which may be of personal nature or has hit her to 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 client with regard to the motive and purpose of collecting such information. There is, therefore, a need for registered intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Registered intermediaries shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

Repeal and Savings

83. On and from the issue of this Circular, the circulars listed out in the Appendix to this Circular shall stand rescinded. Not with standing such rescission, anything done or any action taken or purported to have been done or taken, shall be deemed to have been done or taken under the corresponding provisions of this Master Circular.

Appendix

The following Circulars shall stand rescinded from the date of issuance of this Circular

1. **SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091datedJune16,2023-**

Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT)/ Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

2. **SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/0170datedOctober13,2023-**

Amendment to the Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money-laundering Act, 2002 and Rules framed there under.

3. **SEBI/HO/MIRSD/SEC-5/P/CIR/2023/062 dated April 26, 2023 -** Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries.

4. **SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 –** Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under.

POLICY ON CIRCULATION OF UNAUTHENTICATED NEWS

POLICY ON CIRCULATION OF UNAUTHENTICATED NEWS

The purpose of this policy is to Protect Investors by avoiding/restricting the unauthenticated news circulation related to various scrips by the Company's Employees/Trainee or other dealing person and by company Infrastructure without adequate caution.

It has been observed that market news circulated through blogs/chat forums / email by employees without adequate caution can do considerable damage to the normal functioning and behavior of the market and distort the price discovery mechanisms.

As per code of conduct for Stock Broker in SEBI (Stock Brokers and Sub brokers) Regulations, 1992 and SEBI circular Cir/ISD/1/2011 dated March 23, 2011, all SEBI registered market intermediaries are required to have proper internal code of conduct to govern the conduct of its Employees. In view of same the company implements code of conduct for communicating through various modes of communication. Company Directors/ Officers /Employees/ Trainees are prohibited from:

The Employees of the Company and Trainees are prohibited from

1. Circulation of unauthenticated news related to various Scrip's in blogs/chat forums/emails /websites/social networking sites etc.

2. Encouraging or circulating rumours or unverified information obtained from client, industry, any trade or any other sources without verification

3. Forwarding any market related news received in their official mail/personal mail/blog or in any other manner except after the same has been seen and approved by the Compliance Officer.

4. Employees/temporary staff/voluntary workers etc. employed/working in the offices of market intermediaries do not encourage or circulate rumours or unverified information obtained from client, industry, any trade or any other sources without verification.

5. Access to social media platforms/ instant messaging services/ VoIP / Blogs/Chat forums/ websites/e-mail or any such medium should either be subject to controlled supervision or access should not be allowed.

6. Employees should be directed that any market-related news received by them either in their official mail/personal mail/blog or in any other manner, should be forwarded only after the

same has been seen and approved by the Compliance Officer of the concerned Intermediaries. If an employee fails to do so, he/she shall be deemed to have violated the various provisions contained in SEBI Act and the Rules / Regulations framed thereunder and shall be liable for action. The Compliance Officer shall also be held liable for breach of duty in this regard.

Therefore all the employees of the organization including Directors/ Officers /Employees/ Trainees should follow internal code of conduct and controls of the company.

Employees/Trainees working in the office will not encourage or circulate and therefore restricted to circulate rumors or unverified information obtained from the client, industry and trade or any other sources without verification.

Access Control:
There is no Access to chat forums/ Messenger sites to all the staff. Only senior officials including Directors, Compliance Officer and Senior Manager have the access to the said. All the logs of such sites shall be treated as records and are maintained by the compliance officer. Any information or market related news received by staff in official mail or their personal mail should be forwarded only after the same has been seen and approved by the Compliance Officer of the company.

If an employee fails to do so, he/she shall be deemed to have violated the various provisions contained in SEBI Act/Rules/Regulations etc. and shall be liable for disciplinary action.

This code can be modified/amended/altered as required from time to time in compliance of the relevant provisions/regulations in this regard.

The said Policy has been taken on record and approved by the board of directors of the company at their duly convened meeting held on January 10, 2025.