

PMLA POLICY

FOR

VISHWAS FINCAP SERVICES PVT.LTD

(DP ID –74200)

(Ver. 3.1)

Policy Guidelines on 'Know Your Customer' norms and Anti-Money Laundering measures

Office address: 310, Nangal Raya, Delhi Cant New Delhi-110046

Phone No. 011-47115503, 32008702,

Fax: 011-28113509,

Email: naresh@vishwasonline.com, dp@vishwasfincap.com

PMLA (ANTI MONEY LAUNDERING) POLICY

The VISHWAS FINCAP SERVICES PVT. LTD. has adopted written procedures to implement the anti-money laundering provisions as envisaged under the Anti Money Laundering Act, 2002.

The VISHWAS FINCAP SERVICES PVT. LTD. has adopted guidelines issued by the Securities Exchange Board of India (SEBI) on New Know Your Customer(KYC) standards and Anti Money Laundering(AML) provisions as envisaged under the Anti Money Laundering Act, 2002, which are required to put in place for a comprehensive policy frame work covering KYC Standards and AML Measures.

This policy document is prepared in line with the SEBI guidelines and in line with **The VISHWAS FINCAP SERVICES PVT. LTD.** approach to customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis. The objective of this policy document is to prevent **The VISHWAS FINCAP SERVICES PVT. LTD.** from being used, intentionally or unintentionally, by criminal elements for money laundering activities and for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

PART – I OVERVIEW

1. Introduction:

The Guidelines as outlined below provide general procedures to be followed to ensure the compliance of the guidelines prescribed under the Prevention of Anti Money Laundering Act 2002.

These procedures have been designed considering the specific nature of our business, organizational structure, type of customers and transactions, etc. We all must ensure that the suggested measures and procedures are effectively applied and implemented. The overriding principle is that we should be able to satisfy ourselves that the measures taken by us are adequate, appropriate and we must follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002. (PMLA) and in consideration of SEBI new notification about Know Your Customer (KYC) and Customer Due Diligence (CDD) policies as part of KYC for an effective Anti-Money Laundering process.

2. Back Ground:

The Prevention of Money Laundering Act, 2002, was notified on July 1, 2005. Subsequent to this, the Securities and Exchange Board of India (SEBI) has on 18th January 2006 (Circular Ref. No. ISD/CIR/RR/AML/1/06) required market intermediaries to adopt a policy framework with respect to anti money laundering measures to be followed by the intermediaries.

SEBI vide a master Circular Ref. No. ISD/AML/CIR-1/2008 dated 19th December 2008 directed all registered intermediaries to ensure compliance with the requirements of the Anti Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT)/Obligations of the Security Market Intermediaries under Prevention of Money Laundering Act 2002 and rules framed there- under. Vishwas Fincap Services Pvt. Ltd. is inter alia, a stock broker, a depository participant (DP), a registered intermediary with SEBI and needs to adhere to the same.

VISHWAS FINCAP SERVICES PVT. LTD. has formulated a policy to comply with the SEBI circular. As per the existing policy, Vishwas Fincap Services Pvt. Ltd. has to report to FIU-IND, all market and off market Transactions, inter depository Transactions and Pledge Invocation cases where value of a single transaction total and or series of transaction in single scrip in a month are greater than Rs. 10 lacs. This policy was framed in Dec, 2006. In the present market scenario, it is not practically possible to report every transaction of value Rs. 10 lacs or above. Hence it is felt that we will revise our Anti Money Laundering Policy. Since the business of the Vishwas Fincap Services Pvt. Ltd. has increased, it is necessary to review the same and new measures are taken by the company to form KYC procedures to enable the company to know/understand their customers.

Every transaction in the capital market has two parts i.e. Securities and Funds. Vishwas Fincap Services Pvt. Ltd. deals with the clients only through sub-brokers and Depository Participant (DP) franchises. Therefore, it is difficult for Vishwas Fincap Services Pvt. Ltd. to know about the actual Sources of funds provided to Vishwas Fincap Services Pvt. Ltd. and the Application of the funds issued by Vishwas Fincap Services Pvt. Ltd., in the funds payout on selling of the securities. Monitoring the exact income and net-worth of clients and comparing their transaction value with their income and net-worth are also difficult. Therefore a policy of reporting suspicious Transactions is required to be framed and implemented and to put in place systems and procedures for customer identification and verifying his / her identity, residential address and an online platform that allows investors to complete KYC process online.

OBJECTIVES:

- Ensure that Vishwas Fincap Services Pvt. Ltd. shall meet legal and regulatory obligations, and that its staff is trained properly to and here and comply with prevalent laid down requirements;

- Establish the process of internal control over prevention and detection of accounts and activities falling under the category of suspicious nature by identifying monitoring and reporting to law enforcement authorities;
- Update all subsequent notifications issued by various regulatory authority/exchanges having relevance to the business of intermediary carried on by Vishwas Fincap Services Pvt. Ltd.
- Ensure that the policy/procedures framed are implemented / applied effectively.
- To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.
- To simplify, harmonize the process of KYC with a view to allow ease of doing business in the securities market, by facilitate online KYC(e-kyc)

3. Policies and Procedures to Combat Money Laundering and Terrorist financing.

Guiding Principles

The detailed guidelines in Part II have outlined relevant measures and procedures to guide the registered intermediaries in preventing money laundering and terrorist financing. Considering the specific nature of its business, organizational structure, type of customer and transaction, etc. we should satisfy ourselves that we feel following measures are adequate and appropriate to follow the spirit of the suggested measures in Part II and the requirements as laid down in the Prevention of Money Laundering Act, 2002.

Obligation to establish policies and procedures

U n d e r the Prevention of Money Laundering Act, 2002 as a Securities Market Intermediary, we must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. In order to fulfill these requirements, there is also a need for us to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities

In light of the above, senior management is fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. We therefore:

- (a) Issue a statement of policies and procedures for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;
- (b) Ensure that the content of these Guidelines are understood by all staff members;
- (c) Regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness.
- (d) Adopt customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;
- (e) undertake customer due diligence (“CDD”) measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction;
- (f) develop staff members’ awareness and vigilance to guard against money laundering and terrorist financing

Our Policies and procedures to combat Money Laundering covers:

- a. Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;
- b. Customer acceptance policy and customer 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;
- f. Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

PART II DETAILED OBLIGATIONS

4 Written Anti Money Laundering Procedures

We as securities market intermediary hereby adopt written procedures to implement the anti money laundering provisions as envisaged under the Anti Money Laundering Act, 2002 which includes the following three specific parameters which are related to the overall '**Client Due Diligence Process**':

- a. Policy for acceptance of clients.
- b. Procedure for identifying the clients
- c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

5. KYC Norms

Client Registration Form for each client shall be obtained before opening an account. The company will collect the relevant supporting / proofs and financial information / documents or other Officially Valid document (OVD) as stated in RBI Directions as may be required to establish the genuine identity of the client or the beneficial owners, as the case may be. Annexure attached for the list of OVD.

KYC is strictly reviewed as per aforesaid RBI Directions which provide for identification of ultimate or end beneficiary or controlling power and to take all reasonable steps to identify them.

(A) Facilitation of online KYC

- Implementation of framework that helps KYC process to be completely digital, efficient, compliant, and convenient for customers.
- Providing Facility of Electronic Consent- Electronic consent is the digital equivalent of a physical permission given to the customer/ investors for digital e-KYC by using digital signature (e-Sign) for applicable documents under the provisions of Second schedule of the Information Technology Act.
- Approval of documents for e-KYC consideration In terms of PML Rule 2 (1) (cb) "equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.
- Approval for an online framework of accepting application in online format which as per Section 5 of the Information Technology Act, 2000 recognizes electronic signatures (which includes digital signature)
- In order to enable the Online KYC process for establishing account based relationship with the

RI, Investor's KYC can be completed through online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign.

Framework for E-KYC

The investor visits the website/App/digital platform of Vishwas Fincap Services Pvt. Ltd. fills up the online KYC form and submits requisite documents online.

The name, photograph, address, mobile number, email ID, Bank details of the investor shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under eSign and the same shall be verified by authorized person of Vishwas Fincap Services Pvt. Ltd as under:-

- Mobile and email is verified through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of investor accepted as part of KYC is be the one seeded with Aadhaar or not.
- Aadhaar is verified through UIDAI's authentication / verification mechanism.
- PAN is verified online using the Income Tax Database.
- Bank account details are verified by Penny Drop mechanism or any other mechanism using API of the Bank.

Once all the information as required as per the online KYC form is filled up by the investor/customer, KYC process could be completed as under:

a. The investor/Customer can provide Vishwas Fincap Services Pvt. Ltd. with print out of the completed KYC form and after affixing their wet signature, send the scanned copy / photograph of the same to the office under eSign, or

b. Affix online the cropped signature on the filled KYC form and submit the same to the company under eSign.

“Officially Valid Documents”

In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) “Officially Valid Documents” means the following:

- a. the passport,
- b. the driving licence,
- c. proof of possession of Aadhaar number,
- d. the Voter's Identity Card issued by Election Commission of India,
- e. job card issued by NREGA duly signed by an officer of the State Government and other relevant documents as notified by any other act.

6. Customer Due Diligence

(B) The Customer/Client due diligence (“CDD”) measures comprise the following:

- (a) Obtaining sufficient information in order to identify persons who beneficially own or control 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 should 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.
- (b) Verify the customer’s identity using reliable, independent source documents, data or information;
- (c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;
- (d) Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and
- (e) 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 our intermediary’s knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer’s source of funds.

(C) Verification and Due diligence by KYC Desk:

KYC desk to receive duly filled in Client Registration Docket along with the supporting documents of client and then KYC desk to verify duly filled Client Nirmal Bang Financial Services Pvt. Ltd. 4 Registration Docket with the supporting documents for their completeness in all respects and get it rectified from the client in case of any deficiencies.

ii) Ensure that all the supporting documents and other additional documents are collected and are self attested by the client himself.

iii) In case of Corporate clients, ensure that Resolution of Board of Directors approving the transactions and naming the authorized persons for carrying out the necessary formalities on letter head of the company.

iv) Ensure that corporate client is authorized to enter into loan transaction and carry out the activity for which the loan is being taken as per Memorandum of Association and Articles of Association and should be marked by KYC Desk.

v) While interacting with the Client, KYC desk may conduct due diligence of the client for knowing

the client's background, history, financial status / capability, assessment of business patterns and to verify genuineness of the client.

vi) Cross check PAN details of the client like Permanent Account Number, Name, Father's Name (in case of Individual client), Date of Birth / Incorporation with the details on the website of the Income Tax Department and attach the proof of the same with KYC docket.

vii) In case PAN details are not matching substantially with PAN details printed on PAN Card and PAN details appearing on IT website, take appropriate action to get it clarified from the client. In case of minor discrepancy in the name, obtain the declaration from the client about the same.

viii) Self attested Aadhaar card to be mandatorily collected from each Individual, Authorised Persons, Partners, Directors, Ultimate Beneficial Owner, etc.

ix) Ensure that name filled up in client registration form, Agreement and other document is same as name appearing on PAN card/Aadhaar card. Collect CKYC form if client is not registered in CKYC for sharing information with CKYCR by uploading the KYC data on CERSAI portal. If client is already registered on CKYC, then existing details are verified with the details provided to us. If there is any change in the details, same is updated on the portal and if no change then the existing data is downloaded from CERSAI portal and saved with us in the form of PDF.

x) Under FATCA and CRS, company shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall comply with the reporting requirements as stated in Master Direction – Know Your Customer (KYC) Directions, 2016.

xi) KYC desk should check 'worldcheck', 'watchoutinvestors.com' and SEBI/ Exchange website for client's history and status.

xii) In case of corporate client, ensure that the name of the company is not appearing in the list of vanishing companies as provided on Ministry of Corporate Affairs (MCA) website. Keep the checking detail with the KYC docket.

xiii) In case of default or any action taken by any regulatory authorities against such client is found on verification then seek clarification from the client and co-ordinate with client to find out further details in such default and status as on date.

Policy for acceptance of clients:

The following safeguards are to be followed while accepting the clients:

a) No account is opened in a fictitious / byname name or on an anonymous basis.

- To ensure this we must insist the client to fill up all the necessary details in the KYC form in our presence and obtain all the necessary documentary evidence in support of the information filled in KYC. We must verify all the documents submitted in support of information filled in the KYC form with the originals and in-person verification should be done by our own staff. Moreover new client should either be introduced by an existing customer or by the senior official of the company. In case we have doubt that in-complete / fictitious information is submitted by the client, we must ask for such additional information so as to satisfy our self about the genuineness of the client and the information of the client before accepting his registration.

b) Factors of risk perception of the client:-

Particulars Factors of Risk Perception having regard to :	Risk Perception
Client`s Location (Registered / Correspondence/ other address)	
Face to Face clients of Delhi & NCR	Low Risk
Face to Face clients of other than Delhi & NCR	Low Risk
Client Introduced by existing Face to Face Clients	Low Risk
Client Introduced by other Existing Clients	Medium Risk
Direct Clients of Delhi & NCR	Medium Risk
Direct Clients of other than Delhi & NCR	High Risk
Nonresident Clients	High Risk

Nature of Business Activity, Trading Turnover etc

Particulars	Risk Perception
Retail clients (average daily turnover < Rs 10 Lakhs or net settlement obligation < Rs 2 Lakhs)	Low Risk
Retail clients (average daily turnover Rs.10- 25 Lakhs or net settlement obligation Rs.2-5 Lakhs)	Medium Risk
Retail Clients (average daily turnover > Rs 25 Lakhs or net settlement obligation > Rs 5 Lakhs)	High Risk

Manner of Making Payment

Particulars	Risk Perception
Regular payment through A/c payee cheque from the Bank A/c already mapped with us.	Low Risk

Payment through A/c payee cheque from the Bank A/c other than one already mapped with us.	Medium Risk
Payment through Banker`s Cheque / Demand Draft / Cash	High Risk

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF INDIVIDUALS

Type	Recommended Risk	Risk Perception
Salaried	Low risk	Source on income is fixed and pattern of entries in the account can be correlated with known sources of income/ expenditure
Senior citizens	Medium / High Risk/ Low	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
House-wife	Medium / High Risk/ Low	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O
Self Employed Professionals/ Businessmen	Low risk (except professionals associated with the film industry who will be categorized as "Medium" risk).	Accounts maintained by Chartered Accountants, Architects, Doctors, Lawyers, Sportsmen, etc.
Non Resident Individuals	Low / Medium risk	Transactions are regulated through AD and the accounts are opened only after IPV. In case an IPV is not performed and we have relied on documentation submitted by the client, the account would be categorized as medium risk

Politically Exposed Persons resident outside India	High Risk	Politically exposed persons 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. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Front end staff should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Such accounts should be subjected to enhance monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members and close relatives of PEPs. Further VISHWAS FINCAP SERVICES PVT.LTD. may maintain a list of additional accounts as “Designated PEP” The accounts of Politically Exposed Persons resident
		outside India shall be opened only after obtaining the approval of Business Head. Further, in the event of an existing customer or the beneficial owner of an account subsequently becoming PEP, Business head approval would be required to continue the business relationship and such accounts would be subjected to Customer Due Diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. In such events VISHWAS FINCAP SERVICES PVT.LTD. shall be guided by the information provided by the clients or front end teams.

NOTE: If any of the above accounts are operated by Power of Attorney (POA) holder/mandate holder, then the account will be categorized as “High Risk”, Low/ Medium

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF NON-INDIVIDUALS

Risk categorization of Non Individual customers can be done basis:

A. Type of Entity

Type	Recommended Risk Categorization	Risk Perception
------	---------------------------------	-----------------

Private Ltd/Public Ltd Companies	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such companies would be classified. Such classifications shall be decided post the review of the compliance officer
Local Authorities or Public Bodies	Low Risk/Medium	They are constituted under Special Acts. Operations are governed by such Acts / Rules
Public Sector Undertakings, Government Departments/ Undertakings, Statutory Corporations	Low Risk/Medium	These types of entities are governed by specific Acts, Notifications etc framed by the Government of India or the State Govt and are controlled and run by the Govt.
Mutual Funds/Scheduled Commercial Banks/Insurance Companies/Financial Institutions	Low Risk/Medium	These entities are strictly regulated by their respective regulators
Partnership Firm	Low / Medium / High risk	Depending on the clarity of the shareholding structure and the nature of operations, such entities would be
		classified. Such classifications shall be decided post the review of the compliance officer
Trusts – Public Charitable Trust	Medium / High Risk	Depending on the clarity of the beneficial ownership and the nature of operations, such entities would be classified. Such classifications shall be decided post the review of the compliance officer
Hindu Undivided Family (HUF)	Low Risk/Medium	These are unregistered bodies and the pattern of entries in the account may not be correlated with known sources of income/ expenditure
Societies / Associations / Clubs	High Risk (except 'Housing Societies' which will be categorized as "Low" risk).	These are not highly regulated entities and the pattern of entries in the account may not be correlated with known sources of income/ expenditure
Trusts – Private Trust	High Risk/ Medium	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known sources of income/ expenditure
Co-operative Banks	Medium / High Risk	These are not highly regulated entities

Notes:

1. Lowering of risk classification shall be carried out by the Compliance officer in consultation with the CFO.

This shall be done only where adequate justifications can be provided and the same are mentioned along with the account opening form.

2. Such justifications shall be reviewed 3 months from the date of account opening / first transaction in order to ensure that the classification is proper.
3. Based on the above categorization the transaction review process will take place.
4. Higher Risk Categorization derived from "A"

Client of Special Categories as defined under Para 5.4 of these Guidelines

- b) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.
- c) Ensure that an account is not opened where we unable to apply appropriate clients due diligence measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the intermediary is suspected to be non genuine, perceived non co-operation of the client in providing full and complete information. We should not continue to do business with such a person and file a suspicious activity report. We should also evaluate whether there is suspicious trading in determining whether to freeze or close the account
- d) We should be cautious to ensure that we do not return securities or money that may be from suspicious trades after consulting the relevant authorities in determining what appropriate action should be taken when we suspect suspicious trading.
- e) In case the client proposes to deal through a POA / authorized person we must analyse the circumstances under which the client wish to act on behalf of another person / entity. The authority letter / POA must specify in what manner the account will 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) should be clearly laid down. Adequate verification of a person's authority to act on behalf the customer should also be carried out and all the KYC document of the Agent / POA must be obtained in addition to that of the client.
- f) Necessary checks and verification should be undertaken 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.

Risk-based Approach

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

5.3.2 Risk Assessment:

I -We 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. 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 (these can be accessed at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>).

II- 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.

Clients of special category (CSC):

Such clients include the following-

- a. Nonresident clients.
- b. High net worth clients (Clients having, Net worth \geq 25 Lakh and/or Annual Income exceeding Rs 10 Lakh)
- c. Trust, Charities, NGOs and organizations receiving donations
- d. Companies having close family shareholdings or beneficial ownership
- e. Politically exposed persons (PEP) of foreign origin

f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)

g. Companies offering foreign exchange offerings

h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.

i. Non face to face clients

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

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

Client identification procedure:

The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – 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. Intermediaries shall 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. Further, the enhanced CDD measures as outlined in clause 5.5 shall also be applicable where the beneficial owner of a client is PEP.

b) We 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

c) We 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.

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 to frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices. 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 there under so that the intermediary is aware of the clients on whose behalf it is dealing

We 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 information and 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. PML Rules have recently been amended vide notification No. 13/2009 dated November 12, 2009 and need to be adhered to by registered intermediaries.

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, AMCs etc.) from the 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 intermediaries and non-compliance shall attract appropriate sanctions. Obtaining the minimum information/documents from clients as stipulated in.

Reliance on third party for carrying out Client Due Diligence (CDD):

- i. We rely on a third party for the purpose of (a) identification and verification of the identity of a client

and (b) 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 for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

- ii. 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. Further it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

6. Record Keeping

We must ensure compliance with the record keeping requirements for **5 years** contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

We must 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 behavior.

Should there be any suspected drug related or other 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, we should retain the following information for the accounts of our customers in order to maintain a satisfactory audit trail:

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

All should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities.

We must maintain proper record of transactions prescribed under Rule 3, notified under the

Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:

- (i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (i) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
- (i) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- (iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

7. Information to be maintained

We must maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules:

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

8. Retention of Records

We must maintain and preserve such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities and such record have to be maintained and preserved for a period of 08 years from the date of cessation of the transactions between the client and intermediary.

As stated in sub-section 5.5, We 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 accountfiles and business correspondence shall be maintained and preserved for a period of eight years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later."**, i.e. the date of termination of an account or business relationship between the client and intermediary

Thus the following document retention terms should be observed:

- (a) All necessary records of transactions (namely financial statements, DP Account statements,

Contract Notes, statement of securities etc), for both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

(b) We maintain and preserve the record of documents evidencing the identity of its clients and beneficial owners (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of eight years after the business relationship between a client and intermediary has ended or the account has been closed, whichever 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 should be retained until it is confirmed that the case has been closed.

Records of information reported to the Director, Financial Intelligence Unit - India(FIU-IND):

> We maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of eight years from the date of the transaction between the client and the intermediary.

9. Monitoring of transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. This is possible only if we understand the normal activity of the client so that we can identify the deviant transactions / activities.

We 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/FIUIND/ other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction between the client and intermediary" as is required under the PMLA

We should ensure that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

Further the RMS / Compliance Department should randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions

or not

10. Suspicious Transaction Monitoring & Reporting

We must examine a selection of transaction undertaken by clients on regular basis to enable suspicious transactions as defined in PML Rules as amended from time to time to be recognized and have follow appropriate procedures for reporting suspicious transactions.

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:

- a) Clients whose identity verification seems difficult or clients appears not to cooperate
- b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
- d) Substantial increases in business without apparent cause;
- e) Unusually large cash deposits made by an individual or business;
- f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- g) Transfer of investment proceeds to apparently unrelated third parties;
- h) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicious transaction should be immediately notified to the Money Laundering Control Officer or and the Principle Officer, **Mr.Naresh Kumar Rana** 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 should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should 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.

It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. We must take a note of the same and report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

Clause 5.4(vii) of this Master 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'. Intermediaries are directed that such clients shall also

be subject to appropriate counter measures. These measures may include a 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.

11. List of Designated Individuals/Entities:

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 <http://www.un.org/sc/committees/1267/consolist.shtml>. This is directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. We continuously scans all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIUIND.

12. Procedure for freezing of funds, financial assets or economic resources or related services:

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The obligations to be followed by intermediaries to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Circular ref. no: ISD/AML/CIR-2/2009 dated October 23, 2009, which needs to be complied with scrupulously.

13. Reporting to Financial Intelligence Unit-India

In terms of the PMLA rules, we are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address in the format as prescribed in PMLA Rules:

Director, FIU-IND,

Financial Intelligence Unit-India, 6th Floor,

Hotel Samrat, Chanakypuri, New Delhi-110021.

Website: <http://fiuindia.gov.in>

We should carefully go through all the reporting requirements and formats enclosed with this circular. These requirements and formats are divided into two parts- Manual Formats and Electronic Formats. Details of these formats are given in the documents (Cash Transaction Report- version 1.0 and Suspicious Transactions Report version 1.0) which are also enclosed with this circular. These documents contain detailed guidelines on the compilation and manner/procedure of submission of the manual/electronic reports to FIU-IND. The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also detailed in these documents. In case we are not in a position to immediately file electronic reports, we may file manual reports to FIU-IND as per the formats prescribed. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, we should adhere to the following:

- a) The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.
- (b) The Suspicious Transaction Report (STR) should 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 should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
- (c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
- (d) Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
- (e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported

We should not put any restrictions on operations in the accounts where an STR has been made moreover we all {directors, officers and employees (permanent and temporary)} are prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND to the client at any level

14. Designation of an officer for reporting of suspicious transactions

To ensure that we properly discharge our legal obligations to report suspicious transactions to the authorities, we have already appointed **Mr. Naresh Kumar Rana** as the Principal Officer, who 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.

Appointment of a Designated Director:

i. 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 (be) 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-

- (i) The Managing Director or a Whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
- (i) In terms of Section 13 (2) of the PML Act (as amended by the Prevention of Money-laundering (Amendment) Act, 2012), 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.
- (i) We shall communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND.
- (iv) Designated Directors Mr. Naresh Kumar Rana reporting to FIU related suspicious transaction and other these type transaction.

We are directed to review their AML/CFT policies and procedures and make changes to the same accordingly. The other provisions specified in the SEBI Master Circular dated December 31, 2010 remain the same.

The Stock Exchanges and Depositories are directed to:

a. bring the provisions of this Circular to the notice of the Stock Brokers and Depository Participants, as the case may be, and also disseminate the same on their websites;

- b. makes amendments to the relevant bye-laws, rules and regulations for the implementation of the above decision in co-ordination with one another, as considered necessary;
- c. monitor the compliance of this Circular through half-yearly internal audits and inspections; and
- d. communicate to SEBI, the status of the implementation of the provisions of this Circular

In case of Mutual Funds, compliance of this Circular shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other intermediaries, by their Board of Directors.

This Circular is being issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992 and the Prevention of Money laundering (Maintenance of Records) Rules, 2005 to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

This Circular is available on the SEBI website (www.sebi.gov.in) under the section SEBI Home > Legal Framework > Circulars.

15. Employees' Hiring/Employee's Training/ Investor Education

Hiring of Employees

Having regard to the risk of money laundering and terrorist financing and the size of our business, we have identified various screening procedures to ensure high standards when hiring employees at the key positions and that employees taking up such key positions are suitable and competent to perform their duties.

Employees' Training

We have implemented an ongoing employee training programme so that the members of the frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers are adequately trained in AML and CFT procedures. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

Investors Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. There is, therefore, a need to educate the customer of the objectives of the AML/CFT programme

: REVIEW OF THE POLICY:

The policy shall be reviewed from time to time as and when required by the Management and also implement the change after any change in the Anti Money Laundering Act 2002 or change in any other act, bye-laws, rules, regulations of SEBI, CBI or in any statutory and regulatory Government department related to or affect to this.

Revision

Date	Version	Comment	Authorized
February'2023	3.0	Policy created	Mr. Rajdeep Mandal
February'2023	3.0	Policy verified	Mr. Naresh Kumar Rana
June'2024	3.1	Policy verified	Mr. Naresh Kumar Rana