

Prevention of Money Laundering Policies

Know Your Customer' Guidelines

Anti Money Laundering Standards

1. Know Your Customer Standards

a) The objective of the KYC guidelines is to prevent MANIPUT INVESTMENTS PRIVATE LIMITED (MANIPUT) from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable MANIPUT to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The revised KYC policy of the MANIPUT incorporates the following four elements:

- ✚ Customer Acceptance Policy (CAP)
- ✚ Customer Identification Procedures (CIP)
- ✚ Monitoring of Transactions; and
- ✚ Risk Management

b) A customer for the purpose of KYC Policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the MANIPUT.
- One on whose behalf the account is maintained (i.e., the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Broker, Chartered Accountants, Solicitors, etc as permitted under the law
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the MANIPUT, say, a wire transfer or issue of high value demand draft as a single transaction.

2. Customer Acceptance Policy (CAP)

a) The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in by the MANIPUT. The staff shall accept customer strictly in accordance with the said policy:

- 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 customer and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk called Level I, Level II and Level III

respectively; Customers requiring very high level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as Level IV.

- The staff shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time.
- The staff shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of data/information furnished to the branch. The staff shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the staff shall do so only after permission of Senior Official of their concerned Offices is obtained. Further, the customer should be given a prior notice of at least 20 days wherein reasons for closure of his account should also be mentioned.
- The staff shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. RBI has been circulating lists of terrorist entities notified by the Government of India so that MANIPUT exercise caution against any transaction detected with such entities. The staff shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the MANIPUT are not in any way involved in any unlawful activity and that they do not appear in such lists.

- b) The staff shall prepare a profile for each new customer based on risk categorization. The MANIPUT has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is 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 dealer. The staff should continue to follow strictly the instructions issued by the MANIPUT regarding secrecy of customer information. The staff should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of services to general public, especially to those, who are financially or socially disadvantaged.

c) The risk to the customer 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. The illustrative examples of low risk customers 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 customer shall be met.

⇒ **Medium Risk (Level II):**

Customers that are likely to pose a higher than average risk to the MANIPUT may be categorized as medium or high risk depending on customer'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 a 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.

⇒ **High Risk (Level III):**

The staff may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include

- a) Non Resident Customers,
- b) High Net worth individuals
- c) Trusts, charities, NGOs and organizations receiving donations,
- d) Companies having close family shareholding or beneficial ownership
- e) Firms with 'sleeping partners'
- f) Politically Exposed Persons (PEPs) of foreign origin
- g) Non-face to face customers, and
- h) Those with dubious reputation as per public information available, etc.

The persons requiring very high level of monitoring may be categorized as **Level IV**.

3. Customer Identification Procedure (CIP)

- ✂ Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information. The staff need to obtain sufficient information necessary to establish, **to their satisfaction**, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. Being satisfied means that the dealer is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the staff shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the staff 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 customer and determine who are the natural persons who ultimately control the legal person. Customer Identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure I for the guidance of staff.

- ✂ If the dealer decides to accept such accounts in terms of the Customer Acceptance Policy, the dealer 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(s) is/are. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure - II.

- ✂ Due diligence should be carried out to ensure that no account is opened in a fictitious/benami name or anonymous basis and also verified with the UN list of banned entity, SEBI banned entity list or orders/investigations issued by regulatory authorities/media information.

4. Monitoring & Reporting of Transactions

- ✂ Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account. Staff shall pay special attention to all complex, unusually large transactions an amount of more than Rs. 10 Lacs with the alerts given by the CDSL 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 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 Meeting of the Board on quarterly intervals. 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 customers.

5. Risk Management

- The MANIPUT's KYC policies and procedures covers management oversight, systems and controls, segregation of duties, training and other related matters. For ensuring effective implementation of the MANIPUT's KYC policies and procedures, the staff shall explicitly allocate responsibilities within the branch. The Branch Dealer shall authorize the opening of all new accounts. The staff shall prepare risk profiles of all their existing and new customers and apply Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.
- Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the MANIPUT's policies and procedures to combat money laundering shall be provided to all the staff members of the MANIPUT periodically in phases.
- The Accounts Department shall be empowered to prescribe threshold limits for a particular group of accounts and the staff shall pay particular attention to the transactions which exceed these limits. The threshold limits shall be reviewed annually and changes, if any, conveyed to staff for monitoring.

6. Screening of Employees & Employee training:

- The appointment of employees is done only after they have had a meeting with the director/Head of department of the company.
- The employee is selected only on reference and Walk-in interviews are not conducted and are entertained only through reference.

- Verification is also done as to whether the employee has not been convicted for any offence under any Act prevailing in India
- Proper identification & referencing is done at the time of final appointment of the employee which includes collecting documents on photo-id proof & the address proof

7. Customer Education

Implementation of KYC procedures requires staff to demand certain information from the customers that may be of personal in nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the front desk staff needs to handle such situations tactfully while dealing with customers and educate the customer of the objectives of the KYC programme. The staff shall also be provided specific literature/pamphlets to educate customers in this regard.

8. New Technologies

The KYC procedures shall invariably be applied to new technologies to such other product which may be introduced by the MANIPUT in future that might favour anonymity, and take measures, if needed to prevent their use in money laundering schemes.

Staff should ensure that appropriate KYC procedures are duly applied before issuing the client code to the customers. It is also desirable that if at any point of time MANIPUT appoints/engages agents for marketing of products are also subjected to KYC measures.

While, the revised guidelines shall apply to all new customers/accounts, staff shall apply these to the existing customers 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 Customer Due Diligence (CDD) measures. It has however to be ensured that all the existing accounts of companies, firm, trusts, charitable, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'.

9. Appointment of Principal Officer

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the MANIPUT, Senior Executive heading the Compliance Department of the MANIPUT at Corporate Office shall act as Principal Officer. 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, MANIPUT and any other institutions that are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall furnish a compliance certificate to the Board on quarterly basis certifying that Revised Anti Money laundering Policy is being strictly followed by all the staff of the MANIPUT.

10. Records Maintenance :

- All securities will be / is stored in fire-proof cabinet. All other documents like instruction slips, account opening forms etc. in physical form will be / is stored at the corporate office located in Mumbai, India. Daily backup will be / is taken on DATs/ DVDs will be / is maintained at our premises in a fire proof cabinet. Periodically backup will be/ is taken on DATs/DVDs will be / is store at remote place at the residence of the Director.
- Maintain an efficient system of filing. Physical copies of all documents directly affecting operations will be preserved. All documents on the basis of which data is entered/updated in the system will be preserved. All correspondence between Participant and clients/ Issuer/ R & T agent/trading members/clearing members/companies will be preserved. All the records are to be maintained by the participants for a period of ten years. However in case of ongoing investigations or transactions which have been the subject of STR, they shall be retained for further 10 years from the date closer of case.

Customer 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 customer identification procedures. The staff should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, staff 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, staff 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	Staff need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with MANIPUT. Staff 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 shareholders. But at least promoters, directors and its executives need to be identified adequately.
Client accounts opened by professional intermediaries	When the dealer has 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. Staff may hold 'pooled' accounts managed by professional intermediaries on behalf of Entities like mutual funds, pension funds or other types of funds. Staff should also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockMANIPUT 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

	<p>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 MANIPUT rely on the 'customer 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.</p>
<p>Accounts of Politically Exposed Persons(PEPs) resident outside India</p>	<p>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. Staff 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. Staff should verify the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The staff should seek prior approval of their concerned Heads for opening an account in the name of PEP.</p>
<p>Accounts of non-face-to-face customers</p>	<p>With the introduction of telephone and internet service, increasingly accounts are being opened by MANIPUT for customers without the need for the customer to visit the MANIPUT branch. In the case of non-face-to-face customers, apart from applying the usual customer 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, staff may also require the first payment to be effected through the customer's account if any with another MANIPUT which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the staff 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.</p>

Customer Identification Procedure

Features to be verified and documents that may be obtained from

Customers

Features Documents

Accounts of individuals	<input type="checkbox"/> <input type="checkbox"/> Legal name and any other names used <input type="checkbox"/> <input type="checkbox"/> Correct permanent address (i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the satisfaction of the branch) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch (vii) Telephone bill (viii) MANIPUT account statement (ix) Letter from any recognized public authority (x) Telephone bill (xi) Electricity Bill (xii) Ration Card (xiv) Letter from the employer, (subject to the satisfaction of the branch) (xv) Any other document which provides customer information to the satisfaction of the MANIPUT will suffice.
Accounts of companies	<input type="checkbox"/> <input type="checkbox"/> Name of the company <input type="checkbox"/> <input type="checkbox"/> Principal place of business <input type="checkbox"/> <input type="checkbox"/> Mailing address of the company <input type="checkbox"/> <input type="checkbox"/> 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

	<p>authority to operate the account</p> <p>(iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf</p> <p>(iv) Copy of PAN allotment letter</p> <p>(v) Copy of the telephone bill</p>
Accounts of partnership firms	<p><input type="checkbox"/><input type="checkbox"/> Legal name</p> <p><input type="checkbox"/><input type="checkbox"/> Address</p> <p><input type="checkbox"/><input type="checkbox"/> Names of all partners and their addresses</p> <p><input type="checkbox"/><input type="checkbox"/> Telephone numbers of the firm and partners</p> <p>(i) Registration certificate, if registered</p> <p>(ii) Partnership deed</p> <p>(iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf.</p> <p>(iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses</p> <p>(v) Telephone bill in the name of firm/partners</p>
Accounts of trusts & foundations	<p><input type="checkbox"/><input type="checkbox"/> Names of trustees, settlers, beneficiaries and signatories</p> <p><input type="checkbox"/><input type="checkbox"/> Names and addresses of the founder, the managers/directors and the beneficiaries</p> <p><input type="checkbox"/><input type="checkbox"/> Telephone/fax numbers</p> <p>(i) Certificate of registration, if registered</p> <p>(ii) Power of Attorney granted to transact business on its behalf</p> <p>(iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses</p> <p>(iv) Resolution of the managing body of the foundation/association</p> <p>(v) Telephone bill</p>