PMLA POLICY

FOR

MAGNUM EQUITY BROKING LTD.

DOCUMENT CONTROL PAGE

Document Name	PMLA Compliance Policy

Authorization	Document Owner	Last Reviewed On	Reviewed by	Authorized by
Name	MAGNUM EQUITY BROKING LTD.	10/04/2015	Mr. Sanjay Vora	Mr. Jiten J. Chheda
Signature				

Classification	Distribution List
Official Use Only	Employees/ Sub-brokers/ Authorised Persons/ Branch Heads

All queries, suggestions and changes required may be emailed to sanjay.vora@magnum.co.in (Principal Officer).

INTERNAL CIRCULAR FOR COMPLIANCE WITH ANTI MONEY LAUNDERING PROVISION

PROVISION	RESPONSIBLE DEPARTMENT	ACTION
Customer Due Diligence ➢ **Policy for acceptance of clients:** ➢ **Clients of special category (CSC):** ➢ **Client identification procedure :**	Customer care / Compliance Department	Customer care department with the co-ordination of compliance department will take care of customer due diligence. Client should be categorized into high risk, moderate & low risk.
Record Keeping	Finance & Accounts	Record to be maintained of all Cash transactions above Rs. 10 lakhs. Record of all transactions including suspicious transactions to be maintained in hard / soft copies.
Retention of Records	All Departments.	Records to be maintained for 5 years.
Monitoring of transactions by broking division	Compliance Department	All transaction to be scrutinized and transaction of suspicious nature should be escalated to the principal officer. The principal officer shall take immediate action on all such transaction and report it to FIU IND, in case the client is unable to provide necessary information as to the genuineness of the transaction
Monitoring of transactions by DP division	Demat department/ Compliance Department	The demat department in co-ordination with compliance department shall track the transaction including alerts sent by CDSL. All such transaction to be scrutinized and transaction of suspicious nature should be escalated to the principal officer. The principal officer shall take immediate action on all such transaction and report it to FIU IND, in case the client is unable to provide necessary information as to the genuineness of the transaction
Suspicious Transaction Monitoring & Reporting	Principal Officer	Record to be maintained of payments or transfers received from third parties (other than clients) which are of suspicious nature, if any. Record is to be maintained for transfers which are of suspicious transactions in the Demat accounts.
Designation of an officer for reporting of suspicious transactions	Management & Board of Directors	Board of Directors will appoint principal officer and will intimate to FIU- Delhi
Furnishing of information to the Director (FIU)	All Departments.	The Principal Officer shall furnish the information in respect of transactions referred to in rule 3 every **month** to the Director by the 15th day of the succeeding month

Background:

The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July, 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India. As per PMLA, every banking company, financial institution (which includes Chit Fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and Intermediary (which includes a Depository Participants, Stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, Portfolio Manager, Investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions, the nature and value of which has been prescribed in the Rules notified under the PMLA. For the purpose of PMLA, transactions include:

1. All cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency.

2. All series of cash transactions integrally connected to each other, which have been valued below Rs.10 Lakhs or its equivalent in foreign currency, such series of transactions within one calendar month.

3. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as Demat account, security account maintained by the registered intermediary. For the purpose of suspicious transactions reporting apart from `transactions integrally connected', `transactions remotely connected or related need to be considered. "Suspicions Transactions" means a transaction whether or not made in cash which to a person acting in good faith –

    a. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

    b. Appears to be made in circumstances of unusual or unjustified complexity; or

    c. Appears to have no economic rationale or bonafide purpose.

The Anti-Money Laundering Guidelines provides a general background on the subjects of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to discourage and identify any money laundering or terrorist financing activities.

Prevention of Money Laundering Policies

1. Know Your Customer Standards

a) The objective of the KYC guidelines is to prevent MAGNUM EQUITY BROKING LIMITED (MAGNUM) from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable MAGNUM 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 MAGNUM 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 MAGNUM.
- 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 MAGNUM, 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 MAGNUM. 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.
- 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 SEBI 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. SEBI has been circulating lists of terrorist entities notified by the Government of India so that MAGNUM 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 MAGNUM 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 MAGNUM 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 MAGNUM 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 MAGNUM 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 whose identity could not be established,
(b) High Net worth individuals whose source of income could not be established
(c) Trusts, charities, NGOs and organizations receiving donations,
(d) Companies having close family shareholding or having multi layer corporate structure whose beneficial ownership could not be identified/ established.
(e) Firms with 'sleeping partners'
(f) Politically Exposed Persons (PEPs) of foreign origin
(g) Non-face to face customers
(h) Clients from High risk countries which do not or insufficiently apply the FATF Recommendations and
(i) Those with dubious reputation as per public information available, etc.

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 and all unusual patterns which have no apparent economic or visible lawful purpose. Transactions that are 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 information on Financial Status/income details of clients should be obtained at the time of opening of demat account. Subsequently, Financial Status/income details of clients should be periodically updated in UCC/CDAS/back office etc. Magnum shall identify cases where volume of client's transaction is not commensurate with the known source of income/ networth of the customer. If any abnormality is noticed, Magnum should file STR with FIU-IND.

- Magnum shall update the financial details of customer on annual basis.

- 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 management on half yearly 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.

- Employees, officers and Directors shall ensure strict confidentiality of the STR filed with FIU and shall not be disclosed/ communicated/ tipped off to the customer or any other person.

- Monitoring Process :

  Compliance Officer shall ensure continuous monitoring of the transactions of the Customers to identify suspicious transactions. Following transactions / activities may be identified as Suspicious transactions as notified by SEBI

  a. Cheque towards the investment is issued by payer other than the account holder and the account holder refuses to give declaration that the source of fund is legitimate.
  b. Client is reluctant in providing information.
  c. Investor induces towards non filing of returns or forms to regulatory bodies.
  d. Unusual request is made from the client like not to send account statements.
  e. Sudden increase \ decrease in the number of transactions by the client.
  f. Inoperative accounts suddenly become operative.
  g. There are frequent changes in the address of client.
  h. Documents sent to the client are returned undelivered frequently.
  i. Off Market Transactions insist by the client.
  j. Volume of transaction not commensurate with the known source of income/ networth of the customer.

- Reporting Process :

i. The Member/ DP shall initially register on the portal of FIU-IND and create its login id on https://finnet.gov.in.

ii. All alerts shall be noted in the Suspicious Transaction Register. Further the alerts sent by Exchanges/ Depositories shall also be noted in the Suspicious Transaction Register.

iii. Any suspicion transaction needs to be notified immediately to the "Principal Officer". The notification may be done in the form of a detailed report with specific reference to the client's transactions and the nature or reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told other wise and the client should not be told of the report or suspicion.

iv. 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.

v. Notifications issued by SEBI require STR to be reported within 7 working days of establishment of suspicion at the level of Principal Officer.

vi. Cash Transaction in excess of the threshold limit should also be reported to FIU-IND.

5. Risk Management

- The MAGNUM'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 MAGNUM's KYC polices 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 MAGNUM's policies and procedures to combat money laundering shall be provided to all the staff members of the MAGNUM 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
- Only qualified and competent staff shall be recruited to ensure performance of their duties
- Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the Magnum's policies and procedures to combat money laundering shall be provided to all the staff members of Magnum; periodically in phases. Various case studies and real life situations should be discussed and team members to be educated about the need for implementation of AML guidelines.

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 program. 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 MAGNUM 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 MAGNUM 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. Combating Financing of Terrorism (CFT)-Section 51A of the Unlawful Activities (Prevention) Act, 1967

i. Objective

Vide SEBI Master Circular ISD/AML/CIR-1/2008 dated December 19, 2008 and Circular no.ISD/AML/CIR-1/2009 dated September 1, 2009 on Anti Money Laundering (AML) Standards/Combating Financing of Terrorism (CFT)/Obligations of Securities Market Intermediaries under PMLA, 2002 and Rules framed there-under. Vide paragraph 2 of the Circular dated September 01, 2009, it has been brought to the notice of registered intermediaries that 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 Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Registered intermediaries have been directed that before opening any new account, it will be ensured that the name/s of the proposed customer does not appear in the list. Further, it has been directed that registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities. Full details of accounts bearing resemblance with any of the individuals/entities in the list are required to be intimated to SEBI and FIU-IND.

ii. The Unlawful Activities (Prevention) Act, 1967 (UAPA) was enacted for the prevention of certain unlawful activities of individuals and associations and for matters connected therewith. UAPA has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. The Government has, since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the UAPA, relating to the purpose of prevention of, and for coping with terrorist activities. In terms of Section 51A, 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 and 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.

iii. <u>Implementation:</u>
Principal Officer, on receipt of the updated list of individuals/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities) from the Ministry of External Affairs' through SEBI:

a. should maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with us.

b. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

c. shall send the particulars of the communication mentioned in (b) above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.

d. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011- 23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

e. shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (b) above carried through or attempted, as per the prescribed format.

10. Appointment of Principal Officer

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the MAGNUM, Senior Executive heading the Compliance Department of the MAGNUM 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, MAGNUM and any other institutions that are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall confirm to the management on yearly basis that Anti Money laundering Policy is being followed by all the staff of the MAGNUM.

11. Appointment of Designated Director

To ensure ongoing reporting of compliance with Anti Money Laundering policy of the Magnum, Senior Director at Corporate Office shall be appointed to act as Designated Director. The Principal Officer shall report directly to the Designated Director irrespective of his hierarchy in the organization. Designated Director shall be responsible to report suspicious transactions involving Money Laundering to the Board of Directors. Designated Director shall also be responsible to provide the required information to the regulator(s) as and when demanded/ required under the law.

12. 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 with the clients / Issuer/ R & T agent/trading members/clearing members/companies will be preserved. All the records are to be maintained for a period of five 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 of closer of case.

13. Review of Policy

Designated Director or any other authorized official shall be the authority to give directions for review of the policy and to undertake additions, changes, modifications etc., as directed by SEBI / FIU-IND and all the changes shall be deemed to be incorporated in this policy from their effective date.

14. Program to Test AML Program

The testing of AML program will be performed by the senior Management of the company as a part of internal review/ internal audit. Upon Completion of testing, the finding will be placed before The Board of Directors.

15. Disciplinary Action

A violation of standards, procedures or guidelines established pursuant to this policy shall be presented to Compliance Officer for appropriate action and could result in disciplinary action, including expulsion, dismissal, and/or legal prosecution.

xxxxxxxxxxxxx

Annexure- I

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 MAGNUM. 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 stock MAGNUM 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 MAGNUM 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.
Accounts of Politically Exposed Persons(PEPs) resident outside India	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.
Accounts of non-face-to-face customers	With the introduction of telephone and internet service, increasingly accounts are being opened by MAGNUM for customers without the need for the customer to visit the MAGNUM 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 MAGNUM 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.

Annexure-II

KYC Document collection procedure

1. The Back Office Department shall classify the clients from whom the KYC Documents are to be collected. The client shall be classified on the basis of Type of Customer, Nature of the business, Risk asserted by the client etc.

2. The Back Office Department shall provide the necessary details to the clients regarding registration procedure and submission of relevant documents.

3. In case the requisite documents are not submitted by the prospective client, the department shall follow up with such client through email. The client shall be intimated that the registration shall not be allowed until minimum required documents are submitted.

4. On any default by the client and/ or failure in the submission of the documents the department shall inform the same to the Compliance Officer.

5. The Back Office Department shall request the client to submit the requisite documents within specified period of time. In case the requested document is not submitted by the client, the Back Office Department shall follow up with the client to submit the documents immediately within the grace period.

6. The designated personnel of the Back Office Department shall verify all the documents submitted by the client to confirm its authenticity. Further such personnel shall ensure that all the documents are attested by the client by signature or thumb impression.

7. In case the address as specified in the application is different from that specified in the address proof, the Back Office Department shall thoroughly scrutinize the address proof. The designated personnel shall enquire the reason for above with the Customer. If required, the client shall be insisted to provide the proof for address specified in the application form.

8. Back Office Department shall follow a risk based approach towards certification of documents. In case of low risk customers self attested copies shall be considered sufficient. In case of high-risk customers, the identification documents shall be required to be attested by gazetted officers or notarized by the Notary Public.

9. After verification of the documents, it may be noticed that all the documents may not be provided by the client / prospective client or erroneous documents have been provided by the client. In such case the designated personnel shall immediately intimate the same to the Client by email and telephonic communication.

10. In case the requested document is not submitted by the client, the department shall follow up with the client to submit the documents immediately with the grace period. In case the documents are not submitted by the client, the department shall report the same to the Compliance Officer.