POLICY FRAMEWORK ON ANTI-MONEY LAUNDERING MEASURES

BY A. K. STOCKMART PRIVATE LIMITED

Policy Version: AKSPL/January -2024

Objective

The Objective of this policy framework is to:

- ✓ Create awareness and provide clarity on KYC standards and AML measures.
- ✓ Outline the obligations under Prevention of Money Laundering Act, 2002.
- ✓ Provide a framework for system and procedures.

What is Money Laundering?

Money Laundering is moving illegally acquired cash through financial systems so that it appears to be legally acquired.

There are three common stages of money laundering as detailed below which are resorted to by the launderers and Market Intermediaries which may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions:

1. **Placement** - the physical disposal of cash proceeds derived from illegal activity;
2. **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity;
3. **Integration** – placing the laundered proceeds back into the economy creating the impression of apparent legitimacy to criminally derived wealth.

Using the above methods, the laundered proceeds re-enter the financial system appearing to be normal business funds. Market Intermediaries are therefore placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through the Market Intermediaries. Law protects such disclosures, enabling the person with information to be able to disclose the same without any fear. Market Intermediaries likewise need not fear of breaching their duty of confidentiality owed to customers.

Introduction of Prevention of Money Laundering Act, 2002 (PMLA)

Prevention of Money Laundering Act, 2002 is to combat/ discourage money laundering activities, terrorist financing activities, drug trafficking and other organized and serious crimes. Our policy framework shall be in accordance with PMLA which has come into effect from 1st July 2005 and the necessary Notifications/ Rules have been published in the Gazette of India by the Department of Revenue, Ministry of Finance and Government of India. PMLA is applicable to A. K. Stockmart Private Limited ('AKSPL') - intermediary registered under Section 12 of the SEBI Act, 1992. The framework shall have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

Anti-Money Laundering Program (AML)

In order to discharge the statutory responsibility to detect possible attempts of money laundering, financing of terrorism or any other proceeds of crime, we need to have an AML program that should, at a minimum, include:

I. Businesses Covered by the Code and Background
II. Nature of Transactions
III. Internal policies, procedures, and controls:- Know Your Client Norms of the Company
IV. Identifying and Reporting Suspicious Transactions;
V. Principal Officer;
VI. Record Keeping and Retention of Records;
VII. Hiring and Training Policies;
VIII. Review of the policy.

Written Anti Money Laundering Procedures

Each registered intermediary shall adopt written procedures to implement the anti- money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following 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) Risk Management
d) Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

I. Businesses Covered under this Code of Conduct

This code is applicable to AKSPL which is registered with Securities and Exchange Board of India (SEBI) as a Trading Member and Depository Participants.

II. Nature of Transactions

As prescribed in rule 3 of Prevention of Money-laundering (Maintenance of Records) Rules, 2005, we have to maintain a complete record of certain transactions which includes the nature and value of such transactions. Such transactions include:

1. All cash transactions of the value of more than rupees 10 Lakhs or its equivalent in foreign currency;
2. All series of cash transactions integrally connected to each other which have been individually valued below rupees 10 Lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount an amount of rupees 10 Lakhs or its equivalent in foreign currency;
3. All transactions involving receipts by non-profit organizations of value more than rupees 10 Lakhs, or its equivalent in foreign currency;
4. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

5. All suspicious transactions including attempted 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.
6. All cross border wire transfers of the value of more than INR 5 Lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India;

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

III. Internal Policies and Procedures to combat Money Laundering and Terrorist financing

Know Your Client - Due-Diligence Process

The Client due diligence (CDD) measures comprise of 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, wherever possible. 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 Client's identity using satisfactory evidence, 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 client and/or the person on whose behalf a transaction is being conducted –

I. **For clients other than individuals or trusts:** Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, AKSPL shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

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

Explanation: Controlling ownership interest means ownership of/entitlement to:

- More than 10% of shares or capital or profits of the juridical person, where the juridical person is a company.
- More than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- More than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.
Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

II. **For client which is a trust:** Where the client is a trust, AKSPL shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

III. **Exemption in case of listed companies:** Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

IV. **Applicability for foreign investors:** Dealing with foreign investors' may be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

V. The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half-yearly internal audits. The compliance of the same shall be monitored by the Boards of Directors

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

e) Understand the ownership and control structure of the client.

f) 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 knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and

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

h) AKSPL shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

i) Reliance on third party for carrying out CDD:

i. We may rely on the 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 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 and CDD and record – keeping requirements in line with the obligation under the PML act.

ii. Such reliance shall be subject to the condition 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, we must take accept the ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

Certification of identification documents - Suitable certifiers and the certification procedure

a) Face-to-face

Face-to-face customers can show the Company staff original documents, and copies can be taken immediately and retained. Such copies should be certified by the relevant member of staff of the Company in the manner described above.

b) Non face-to-face

Where it is impractical or impossible to obtain sight of original documents, a copy is acceptable where it has been certified as being a true copy of the original document belonging to the applicant for business in accordance with the certification procedure described above.

c) Persons without standard identification documentation

- **Direct corporate clients**

Corporate structures, financial market intermediary, or being provided with financial services by another regulated entity, are one of the most likely vehicles for money laundering.
Generally, in the case of all types of trusts, if practical, the Company should obtain and verify the identity of any principal beneficiaries

- **Non-profit organizations**

With regard to Recommendation 8 of the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing, the Company should carry out extra due diligence enquiries on non-profit organizations which have established or are seeking to establish a business relationship. The Company should be especially vigilant for unusual transaction patterns or sizeable transactions, and take care to ascertain the geographical activity and business partners of such organizations.

d) Politically Exposed Persons (PEPs) and other high risk customers

There has been much international attention paid recently to "politically exposed persons" (or "potentate") risk, the term given to the risk associated with providing financial and business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their governments and society. This risk is even more acute where such

countries do not have anti-money laundering standards, or where these do not meet international financial transparency standards.

"Politically exposed persons" will include senior political figures and their immediate family, and close associates. The Company would take adequate care in dealing with such client and obtain necessary disclosures, wherever practical.

AKSPL shall be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

a) An appropriate risk management system put in place to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.
b) The prior written approval shall be obtained from senior management/ Principal Officer 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, AKSPL shall obtain senior management/ Principal Officer Approval to continue the business relationship.
c) AKSPL 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 AKSPL by using reliable sources including documents/ information. AKSPL 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 AKSPL 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 AKSPL.

Source of funds and source of wealth

When entering into a business relationship of any type, the Company should consider making enquiries to ascertain the source of wealth of the applicant for business. This information will form part of the overall know your customer profile which the Company must establish for each class of customer as may be laid down from time to time.

The Company would not normally accept generic descriptions of the source of wealth from customers, such as "savings", "investments", "inheritance", or "business dealings", without undertaking further checks to establish the true information behind the generic description. (The generic descriptions mentioned are not exhaustive, and the Company should be vigilant for other generic statements not listed). Such information is central to the concept of knowing the customer, and failure to establish meaningful information about the customer's circumstances may be interpreted by the Company as a failure to properly apply the Know Your Customer principle.

Policy for acceptance of clients

This is to identify the types of clients that are likely to pose a higher than average risk of money laundering or terrorist financing. Through this, we will be in a better position to apply client due diligence on a risk

sensitive basis depending on the type of client business relationship or transaction. The following safeguards are to be followed while accepting the clients:

a) No account shall be opened in a fictitious/ benami name or on an anonymous basis. Accounts for to be opened only after In-Person-Verification (IPV).

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the clients can be identified with regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. Based on the parameters, we should be able to classify the clients into low, medium and high risk. Clients of special category may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile.

c) Documentation requirement and other information shall be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement of PML Rules, directives, circulars, guidelines issued by SEBI from time to time.

d) We shall ensure that an account shall not be opened where we are unable to apply appropriate CDD measures/ KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided is suspected to be non-genuine, perceived non-cooperation of the client in providing full and complete information. We shall not continue to do business with such a person and file a suspicious activity report. We shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. Subject to the regulatory guidelines prevailing in the country, we shall ensure that securities of money that may be from suspicious trades are not returned to the client. However, we shall consult the relevant authorities in determining the action to be taken when we suspect suspicious trading.

e) We shall find out the circumstances under which the client is acting on behalf of another person/ entity. The account shall be operated in a specified manner like 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 us, as well as the person on whose behalf the agent is acting shall be clearly mentioned). Adequate verification of a person's authority to act on behalf the Client shall also be carried out.

f) Necessary checks and balance shall be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

g) The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

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 We ensure that accounts are not opened in the name of anyone whose name appears in said list. We shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

Procedure of 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.

In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide Ministry Order No. 17015/10/2002-IS-VI dated August 27, 2009. After the reorganization of the Division of Ministry of Home Affairs, the administration of UAPA and the work relating to countering of terror financing has been allocated to the CTCR Division (‘Counter Terrorism and Counter Radicalization Division’) and the said order is modified accordingly. We shall ensure effective and expeditious implementation of the procedure laid down in the said order which is listed as below:

a) 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 (MHA)’; SEBI will forward the same to stock exchanges, depositories and registered intermediaries (includes stock broker) for the following purposes:

   i. To 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 them.

   ii. In the event, particulars of any of customer/s match the particulars of designated individuals/ entities, stock exchanges, depositories and intermediaries 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 on their books to the Joint Secretary (CTCR), 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 jsctcr-mha@gov.in

iii. Stock exchanges, depositories and registered intermediaries (includes stock broker) shall send the particulars of the communication mentioned in (ii) 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.

iv. In case the aforementioned details of any of the customers match the particulars of designated individuals/ entities beyond doubt, stock exchanges, depositories and registered intermediaries (includes stock broker) would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (CTCR), 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 jsctcr-mha@gov.in

v. Stock exchanges, depositories and registered intermediaries (includes stock broker) shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by aforesaid carried through or attempted, as per the prescribed format.

b) On receipt of the particulars as aforesaid, CTCR Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/ entities identified by the stock exchanges, depositories, registered intermediaries (includes stock broker) are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by stock exchanges, depositories, registered intermediaries are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

c) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under Section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned depository under intimation to SEBI and FIU-IND. The order shall take place without prior notice to the designated individuals/entities.

We also check the SEBI debarred entity or ban entity or person on regular basis (as and when received) & also check from our existing client list. If we found them in the existing client list then we immediately deactivate the account or take appropriate action/ measures as applicable/ instructed.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001

U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and

entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for CTCL Division for freezing of funds or other assets.

The UAPA nodal officer of CTCL Division of MHA, shall cause the request to be examined, within 5 working days, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators, FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/ entities.

Upon receipt of the requests by these nodal officers from the UAPA nodal officer of CTCL Division, the procedure as enumerated at aforementioned paragraphs shall be followed.

The freezing orders shall take place without prior notice to the designated persons involved

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned stock exchanges/ depositories and registered intermediaries. The stock exchanges/depositories and registered intermediaries shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of CTCR Division of MHA within two working days. The Joint Secretary (CTCR), MHA, being the nodal officer for CTCR Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and registered intermediaries. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of CTCR Division shall inform the applicant.

Risk – based Approach

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

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

Risk Assessment

a) Risk assessment shall be carried out 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 the URL –
http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml
http://www.un.org/sc/committees/1988/list.shtml

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

Clients of special category (CSC)

CSC shall include the following:

a) Non-resident clients;
b) High net worth clients;
c) Trust, Charities, NGOs and organizations receiving donations;
d) Companies having close family shareholdings or beneficial ownership;
e) Politically exposed persons (PEP);
PEP are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc. Further, family members or close relatives of PEPs shall also be considered as CSC and all the measures apply to PEP shall also be apply to them.
f) Companies offering foreign exchange offerings;
g) Clients in high risk countries;
While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, AKSPL apart from being guided by the Financial Action task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to.

However, this shall not preclude AKSPL from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas.

h) Non face to face clients;
i) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and AKSPL shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

If High risk clients,

a) We shall have a provision in the system which continuously check the client's trading patterns;
b) System shall keep a log of deviation from normal trading pattern;
c) System shall check Peaks in trading patterns with clients known financial profile.

Necessary checks and balance are put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide. The client's details are checked with list of banned entities as published by SEBI. Further the clients details are checked from thewebsite http://www.un.org/sc/committees/1267/consolist.shtml and other related sites to verify whether the client belongs to banned entities or barred entities list.

Risk Management & Surveillance Team

Risk Management & Surveillance Team (RMS) gives exposure to clients based on margin available in the system and clean exposure to selected clients based on recommendations of the Business Managers. It is also the duty of RMS to validate such exposures with the financial details provided by the client in KYC forms. Where there is a trading activity of the client, which is not commensurate with the financial details declared by the client, it should be analyzed and referred to the Principal Officer with reasons of suspicion.

Cash Transactions

As a policy we do not accept cash against settlement and or margin obligations for dealing in securities. All payments must be received from the clients strictly by account payee crossed cheques drawn in favour of the Company or through NEFT/RTGS from client`s designated bank account only.

Periodical update

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

The details provided by the clients are updated periodically to ensure that the trades done by the client are consistent with the profile of the client. Financial details of the client are periodically updated. Personal details like e-mail id, phone number, address, bank etc are also updated on regular basis as and when request for updation is received from client.

Monitoring & Reporting of Suspicious Transactions:

Counterfeit Currency Reports:

Monitoring and Reporting to FIU-IND where any forgery of a valuable security or a document has taken place facilitating the transactions with us by any client.

Cross Border Wire Transfer Reports:

Monitoring and Reporting FIU-IND of all cross border wire transfers of the value of more than INR 5 Lakhs or its equivalent in foreign currency by our clients where either the origin or destination of fund is in India.

Client identification procedure based on 'Know Your Client' (KYC) policy:

a) The CIP to be carried out at different stages i.e. while establishing the relationship with client, 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. There shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures.

b) Our normal KYC document shall become a part of our procedures which helps us in due diligence. The KYC team shall adhere to the information required in the client registration form and take all the relevant documents at the time of opening of the account as per the documents enclosed. Each original document shall be seen prior to acceptance of a copy.
   - ✓ A copy of general instruction and check-list of documents for fulfilling requirements in the Client registration kit (in KYC Form)
   - ✓ A copy of general instruction and check-list of documents for fulfilling requirements in the trading/ depository account opening.
   - ✓ A copy of Member client registration form for opening a broking account/ trading account. (in KYC Form)
   - ✓ A copy of Application form for opening a depository account.

c) Account opening team shall call up and send a welcome kit to all the new clients and thus verifying their address and contact details.

For existing clients processes could include -

a. Review of KYC details of all the existing active clients in context to the PMLA requirements.
b. Classification of clients into high, medium or low risk categories based on KYC details, trading activity etc. for closer monitoring of high risk categories etc.
c. Obtaining of annual financial statements from all clients, particularly those in high risk categories.
d. In case of non-individuals additional information about the directors, partners dominant promoters, major shareholders to be obtained.

IV. Identifying and Reporting Suspicious Transactions

What is a Suspicious Transaction?

Suspicious transaction means a transaction including an attempted 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 an offence specified in the Schedule to PMLA regardless of the value involved; or
b) Appears to be made in circumstance of unusual or unjustified complexity; or
c) Appears to have no economic rationale or *bona fide* purpose; or
d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

Identifying such transactions

All the transaction mentioned under clause II of this policy and rule 3 of Prevention of Money-laundering (Maintenance of Records) Rules, 2005 as amended from time to time.

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) Repeated high value cash transactions;
b) Frequent transfer of shares from one Beneficiary owner account to another Beneficiary owner account;
c) Trading beyond the capacity i.e. based on the declared income in KYC/ Balance sheet/ known assets/ personal knowledge etc.;
d) Clients whose identity verification seems difficult or client appears not to cooperate;
e) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing/ business activity;
f) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
g) Substantial increases in business without apparent cause;
h) Unusually large cash deposits made by an individual or business;
i) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
j) Transfer of investment proceeds to apparently unrelated third parties;
k) 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.

Monitoring of Transactions

a) Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. For that we shall have an understanding of the normal activity of the client and then we can identify the deviant transactions/ activities.

b) We shall pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. We shall allow each class of clients to trade based on internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these

limits. The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/ stock exchanges/ FIU-IND/other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction between the client and AKSPL.

c) We shall ensure a record of transaction is preserved and maintained in terms of section 12 of the PMLA (i.e. for a period of five years from the date of transaction between a client and the AKSPL) and that transactions of a suspicious nature or any other transactions notified under Section 12 of PMLA are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the Principal Officer within the organization.

d) The compliance department shall randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are suspicious transactions or not.

Suspicious Transaction Reporting

Any suspicion transaction shall be immediately notified to the Principal Officer. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature/ reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

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

The 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' 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.

Reporting to Financial Intelligence Unit-India

In terms of the PML rules, we shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:
Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

The reporting requirements and formats that is available on the website of FIU–IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format (https://fiuindia.gov.in/files/downloads/Filing_Information.html). These documents contain detailed directives on the compilation and manner/procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, we shall adhere to the following:

a) The cash transaction report CTR (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month;
b) The Suspicious Transaction Report (STR) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion;
c) The Non-Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month.
d) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
e) Utmost confidentiality shall be maintained in filing of CTR and STR to FIU-IND.
f) **No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.**

AKSPL shall not put any restrictions on operations in the accounts where an STR has been made. AKSPL and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

It is clarified that the AKSPL, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, shall file STR if AKSPL have reasonable grounds to believe that the transactions involve proceeds of crime.

No Tipping Off

An important element to the success of the AML process is that the Clients should not be informed (i.e. tipped off) that his/her accounts are being monitored for suspicious activities and / or that a disclosure has been made to the designated authority namely Financial Intelligence Unit, India. (FIU-IND) The Company can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the Client arouse suspicion.

Where it is known or suspected that a suspicion report has already has been made internally or externally, and it then becomes necessary to make further enquiries, care must be taken to ensure that the suspicion is not disclosed either to the client or to any other third party. Such enquiries shall normally be made as directed by the Principal Officer. "Tipping Off' provisions extended not only to the filling of the STR and/or related information but even before, during and after the submission of STR.

V. Principal Officer

We have appointed **Mr. Ashit Raja as a Principal Officer** in order to ensure proper discharge of our legal obligations to report suspicious transactions to the authorities. The Principal Officer will 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. All high risk clients /suspicious transactions/ money laundering activities shall be reported to him and he along with compliance and surveillance team and after consulting the Management of the Company shall do due diligence/ investigation and accordingly necessary steps shall be taken.

VI. Record Keeping and Retention of Records

Record Keeping

a) We shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

b) We shall maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

c) 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 shall retain the following information for the accounts of the clients in order to maintain a satisfactory audit trail:
   i. the beneficial owner of the account;
   ii. the volume of the funds flowing through the account; and
   iii. for selected transactions:
      a. the origin of the funds;
      b. the form in which the funds were offered or withdrawn e.g. cash, cheques, etc.;
      c. the identity of the person undertaking the transaction;
      d. the destination of the funds;
      e. The form of instruction and authority.

d) We shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, we shall consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

Retention of Records

- The following document retention terms should be observed:
  (i) All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act (PMLA as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars. PMLA stipulates that all records shall be maintained for a period of five years from the date of the transaction between the clients and the intermediary.
  (ii) Records evidencing the identity of 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 shall also be maintained and preserved for the period of five years after the business relationship with client ends 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 shall be retained until it is confirmed that the case has been closed.

Maintenance and Preservation of records

Information to be maintained for the transactions reported

a) the nature of the transactions;
b) the amount of the transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted;
d) The parties to the transaction.

Our records and information are properly maintained and preserved in an in-house storage area that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records have to be maintained and preserved for a period of five years from the date of cessation of the transactions between the client and us. The records of the identity of clients have to be maintained and preserved for a period of five years from the date of cessation of the transactions between the client and us.

We shall ensure that the implementation of policy on Anti Money Laundering Measures is the responsibility of the entire organization. It will apply across all aspects of our operations. Our commitment to the above mention policy will be demonstrated in terms of employee accountability, monitoring and auditing programs, training and technology.

We shall follow all above very strictly and to the best of our ability in order to prevent money laundering activities.

However, notwithstanding anything contain in this policy, we shall preserve the following records and documents for minimum period of **EIGHT YEARS** (pursuant to Regulation 66 of the Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018:

a) records of all the transactions entered into with a depository and with a beneficial owner;
b) details of securities dematerialized, rematerialized on behalf of beneficial owners with whom it has entered into an agreement;

c) records of instructions received from beneficial owners and statements of account provided to beneficial owners; and
d) Records of approval, notice, entry and cancellation of pledge or hypothecation, as the case may be.

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

Training, Awareness and Staff Screening

The Company should ensure that all appropriate staff such as frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients, receive training on money laundering prevention on a regular basis, ensure all staff fully understands the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

High standards in hiring policies and training with respect to anti-money Laundering

We have a clear recruitment policy. We shall have adequate screening procedures in place to ensure high standards when hiring employees. We shall obtain references from the employee and cross verify their details from their previous organizations. Thus keeping a check on employee's status and integrity.

We shall identify the key positions within the organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties. We must provide proper anti money laundering and anti-terrorist financing training to our staff members.

Compliance Function

The business objectives of customer care are closely aligned to the regulatory objectives of the KYC principle. Similarly linked are the philosophies of Compliance Function behind the regulatory objectives of protecting the financial integrity of the nation, the commercial desirability of protecting the reputation of individual corporations, and the requirement for effective risk management and good standards of corporate governance.

Investors Education

Implementation of AML/CFT measures requires back office and trading staff 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 client with regard to the motive and purpose of collecting such information. There is, therefore, a need for the back office and trading staff to sensitize their client about these requirements as the ones emanating from AML and CFT framework. The back office and trading staff should prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT programme.

Questions to ask yourself

The following factors should be borne in mind when seeking to identify a suspicious transaction:-

a) Is the customer known personally? ;
b) Is the transaction in keeping with the customer's normal activity known to the Company, the markets in which the customer is active and the customer's own business?;
c) Is the transaction in keeping with normal practice in the market to which it relates i.e. with reference to market, size and frequency?;
d) Is the role of the agent involved in the transaction unusual?
e) Is the transaction to be settled in the normal manner?
f) Are there any other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or to other destinations or beneficiaries?; and
g) Can you understand the reason for the transaction i.e. is there an easier, cheaper or more convenient method available?

Compliance Culture- Vigilance

Vigilance and an enquiring and questioning culture will reduce the risk of the Company's businesses, and indeed staff, becoming the victims of criminals who launder money.

Appointment of Designated Director

In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

"Designated director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes –

a) the Managing Director or a Whole-Time Director duly authorizes by the Board of Directors if the reporting entity is a company,
b) the managing partner if the reporting entity is a partnership firm,
c) the proprietor if the reporting entity is a proprietorship firm,
d) the managing trustee if the reporting entity is a trust,
e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
f) Such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above."

In terms of Section 13 (2) of the PMLA, the Director, FIU–IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

The Board of Directors has appointed **Ms. Annu Garg as the Designated Director** under PMLA & PML Rules. The Designated Director of the Company is also required to ensure the compliances under PMLA.

VIII. Review of the Policy

This policy is reviewed on yearly basis or as and when any new circular(s)/ master circular issued by the SEBI or Stock Exchanges or Depositories etc., with regard to testing its adequacy to meet the compliance requirements of PMLA. The Principal Officer is the authority to give directions to undertake additions, changes, modifications etc. as directed by SEBI/ FIU-IND.

Policy framed by:	Company Secretary – Ms. Sneha Chandan
Policy reviewed by:	Designated Director – Ms. Annu Garg
	Principal Officer – Mr. Ashit Raja