SHRIRAM INSIGHT SHARE BROKERS LTD
Policy on Anti Money Laundering

Version 1.1.17 Dated August 2026

1.1 Background:-

World over, the fight against money laundering (ML) and financing of terrorism has become the topmost priority. ML poses, a risk to the soundness and stability of financial institutions and financial systems, increased volatility of international capital flows, and a dampening effect on foreign direct investment. It is not only shaken the world economy but also threatened the stability of human civilization. Protecting the integrity and stability of the international financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities are some of the measures taken in this regard.

In India, there had been Laws and Regulations for quite some time to address certain aspects of Prevention of Money Laundering (PML), like Criminal Law Amendment Ordinance, 1944 for attachment of proceeds of certain crimes. However, consolidated Anti-money laundering specific legislation, Prevention of Money Laundering Act (PMLA), 2002, came in to effect with the Government of India Gazette Notification on 1st July, 2005. The Financial Intelligence Unit-India (FIU-IND) constituted by Government of India on 18th November, 2004 as a Nodal Agency in India for the Anti-money Laundering (AML) measures and get statutory recognition on and from 1st July, 2005.

Since 2005, there have been a number of developments in the AML/Combating of Financing of Terrorism (CFT) internationally and within India. Therefore, it has become necessary to review and revise the Guiding Notes by incorporating new developments to serve as a reference document to the Stock Brokers in all KYC/AML/CFT issues, especially with India becoming a member country in Financial Action Task Force (FATF) on June, 2010. Shriram Insight Share Brokers Limited as Financial Intermediaries for its Stock Broking, Commodity Futures Broking & DP services came under the purview of PMLA compliance.

It is to be noted that both KYC and AML are integrated and interrelated. Our AML Policy based on the guidelines of the Controlling Authorities such as SEBI (Security Exchange Board of India) circular Ref. No. ISD/CIR/RR/AML/1/06 DATED JANUARY 18, 2005, SEBI circular ref no.ISD/AML/CIR-1/2008 dated December 19, 2008 and Circular No.NSE/INVG/2008/223 dated 22nd December 2008.

SEBI in its circular ISD/AML/CIR-1/2009 Dated 1st September 2009 highlighted the need of more elaborate scrutinizing transactions of Special category clients and the requirements of checking updated list of Individuals and entities whose account has been freezed, and who are subject to various sanctions measures, from designated website, before opening of account of clients.

The policy will be reviewed yearly and as and when required by the relevant authority. Any amendments thereof; will be included in the same to bring it in line with the amendments made in the Act and the Rules framed there under and any other notifications and/or guidelines issued by SEBI. The same will also be placed before board for their noting.

1.2 Objectives:-

Shriram Insight Share Brokers Limited, a leading private sector intermediary in the securities market and commodity future market in India has great culture & highest order of regulatory compliance. It has system to comply with established laws and regulations in order to protect the good name and reputation, reduce the likelihood of becoming a victim of fraud or illegal activity and ensure safe and sound business practices for its customers.

In keeping with our Mission, Values and Policy, we strictly observe laws of the Land and refuse to aid those who attempt to evade them.

In the recent time Money Laundering and Terrorist Financing is a serious threat to financial system of all countries and it leads to destruction of the country's sovereignty and character. This has been widely recognized at the international level.

SISBL had undertaken a comprehensive AML Policy for preventing Money Laundering and Terrorist Financing. The key AML objectives of SISBL are:

To prevent our business channels/products/services from being used as a channel for ML.

- To establish a framework for adopting appropriate AML procedures and controls in the operations/business process of SISBL.
- To lay down AML compliance norms for the employees of the SISBL.

- To ensure compliance with the laws and regulations in force from time to time.
- To protect SISBL reputation.
- To assist law enforcement agencies in their effort to investigate and track money launderers.

2. Regulatory Frame Work

2.1 What is Money Laundering?

The offence of Money Laundering has been defined in Section 3 of the Prevention of Money Laundering Act (PMLA), 2002 as "whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

"Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. The proceeds of crime laundered by criminals often are generated in very heinous crimes like drug trafficking, trafficking in women and children, child pornography, extortion, murder, etc.

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert an institution to criminal activity-

- **Placement**- the physical disposal of cash proceeds derived from illegal activity.
- **Layering**- separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- **Integration**- the provision of apparent to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

Prevention of Money Laundering, therefore, is not only a statutory or

regulatory requirement but also a moral responsibility for all the Financial Intermediately as any facilitation of money laundering indirectly supports these criminal activities.

2.2 Terrorist Financing

Terrorists use similar methods as Money Launderers for moving their funds. Some of the terrorist groups also indulge in criminal activities for generating funds for their activities and some of them are even known to have strong relationships with criminal gangs. The two major differences between terrorist financing and money laundering are:

- Terrorist funding can happen from legitimately obtained income whereas the source of money in money laundering is always from illegal source.
- More often terrorist activities require small amounts and hence it is increasingly difficult to identify terrorist funding transactions since money laundering is always with high value.

2.3 Other Financial Crimes

Other financial crimes such as Fraud and market abuse (insider trading) are closely related to money laundering and terrorist financing and most often the measures described in these guidelines for preventing money laundering and terrorist financing may help financial institutions in preventing fraud and other financial crimes, as well.

2.4 International Developments & Recommended Standards.

2.4.1 Financial Action Task Force (FATF)

One of the most important events to influence international money laundering prevention efforts was the establishment of FATF by the G-7 Summit in 1989 consisting of the G-7 member states, the European Union and Eight other countries. Over the years more members were admitted to the FATF and the current membership is 36, including 34 member states and 2 Regional Organizations, European Union and Gulf Development Council. India has been accorded membership status in June, 2010.

3. Legislation & Regulation in India.

3.1 Prevention of Money Laundering Act. (PMLA), 2002

The first step in the AML legislation in India was the introduction of the PML Bill, 1998 in the Parliament in August 1998. Since the Lok Sabha was dissolved in April, 1999, this bill could not be passed. Prevention of Money Laundering Bill, 1999 was introduced in the Parliament in October, 1999. This Bill was passed by the Parliament in 2002 and received President's assent on January 2003 and PMLA, 2002 was enacted. This law came to effect on 1st July, 2005 after an amendment.

The Act criminalizes money laundering and also provides for freezing and confiscation of assets concerned in money laundering. Appointment of various authorities including Financial Intelligence Unit (FIU) is also covered in its provisions. The Act also lays down obligations of banks in maintaining records of certain prescribed transactions and reporting such transactions to FIU-IND. This also lists out the prescriptive offences, which will come under the purview of the Act.

3.2 Prevention of Money Laundering (Amendment) ACT (PMLA), 2009

Prevention of Money Laundering (Amendment) Act 2009 was duly notified in March, 2009. The key amendments are listed as under**:**
The Act incorporates additional categories of offences punishable under PMLA.

- The Act extends coverage to additional categories of reporting entities such as money remittance business/intermediaries, casinos & dealers in foreign currency authorized under FEMA. The Act also provides authority to the Government to extend coverage to other entities.

- Separate categories of offences with cross-border implications have been defined.

3.3 Prevention of Money Laundering (Amendment) Act. (PMLA), 2012

In terms of Prevention of Money Laundering (Amendment) Act, 2012 enforced from 15th February, 2013, some amendments, substitutions and insertions have been made. The major changes related to reporting entity like Bank are as follows:

- Every Reporting entity shall maintain a record of all transactions, including information relating to transactions in such a manner as to enable it to reconstruct individual transactions;

- Every Reporting entity shall furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;

- Every Reporting entity shall verify the identity of its clients in such a manner and subject to such conditions, as may be prescribed;

- Every Reporting entity shall identify the beneficial owner, if any, of such of its clients, as may be prescribed;

- Every Reporting entity shall maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

- Every information maintained, furnished or verified shall be kept confidential and maintained for a period of five years. Further, in terms of Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 notified on October 03, 2018, Depository Participants are required to preserve the records and documents for a minimum period of eight years.

For the purpose of implementing the provisions of this Act, the Central Government may, in consultation with the Regulator/s prescribe the procedure and the manner of maintaining and furnishing information by a reporting entity.

Section 13(2) of this Act provides the powers of Directors to impose fine if the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may –

a) issue a warning in writing ; or

b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

c) direct such reporting entities or its designated director on the Board or any

of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

d) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

The Act also amended some schedule of its punishable offences.

3.4 Amendment to Prevention of Money Laundering (Maintenance of Records) Rules, 2013

In terms of Prevention of Money laundering (maintenance of Records) Rules, 2013, some amendments and additions have been made. The major changes related to reporting entity like Stock Brokers are as follows:

1) Nomination of Designated Director;
2) Acceptance of Officially valid documents for customer identification;
3) Amendment in definition of transactions:

'Transaction' means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

i. opening of an account;
ii. deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non- physical means;
iii. the use of a safety deposit box or any other form of safe deposit;
iv. entering into any fiduciary relationship;
v. any payment made or received in whole or in part of any contractual or other legal obligation;
vi. any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and
vii. establishing or creating a legal person or legal arrangement.

4) Enhanced or Simplified measures to verify the identity of low-risk customers;

5) Amendment in definition of Cash transaction reporting;

6) Reporting of Cross Border Wire Transfers (CWTR);

7) Amendment in Maintenance of information in respect of transactions;

8) The records of the identity of clients shall be maintained in the manner specified by its regulators ;

9) Identity of Designated Director;

10) Amendment in time schedule for reporting CCR;

11) Customers Delay in reporting a transaction;

12) Verification of identity of low-risk;

13) Reliance on third Party Due Diligence for the purpose of identifying and verifying the identity of customers;

14) Procedure for determining beneficial owner: where the client is a company, the beneficial owner is the natural person, who, whether acting alone or together, or through one or more juridical person(s),

15) Has a controlling ownership interest or who exercises control through other means.

16) Proof of identity and address required at the time of opening an account for Individual, Companies, Partnership firms, Trust & Foundations and Unincorporated Association.

3.5 Rules under PMLA.

In terms of the section 73 of PMLA, the Central Government has been empowered to formulate rules for implementing the provisions of the Act. The rules are notified and published through Official Gazette.

Consequent to the PMLA coming into effect and notification of the rules framed there under, detailed instructions have been issued by the Regulators regarding the responsibilities of regulated entities under the Act, especially on the following points:

- Nomination of Designated Director;
- Appointment of Principal Officers;
- Reporting of Cash Transactions (CTR) above INR ten lakh or its equivalent in foreign currency in a month;
- Reporting of Counterfeit Currency Notes and forged valuable securities detected in a month;
- Reporting of all transactions involving receipt by Non-profit organization (NPO) in a month,
- Reporting of all Suspicious Transactions Report (STR) within 7 days of arriving at a conclusion that any transaction is of suspicious nature;
- Report of transactions of all Cross Border Wire Transfers of the value of more than five lakh rupees (or equivalent in foreign currency) where either the origin or destination of fund is in India.

3.5.1 Anti-Money Laundering (AML) Guidelines for related activities.

There are specific guidelines issued by SEBI for complying with the requirements of PMLA related activities which the Financial Institutes undertake, such as performing due diligence on their customers, maintenance records, monitoring and reporting of suspicious activities to FIU-IND, maintaining records of prescriptive transactions etc.

3.6 Other aspects relating to Anti Money Laundering Measures:

In order to check the money laundering, certain precautionary measures should be adopted. Before entering into an agreement with the prospective customer, following key elements of KYC norms are to be followed:

- Customer Acceptance Policy;
- Customer Identification Procedures;
- Monitoring of Transactions; etc.

3.6.1 Customer Acceptance Policy (CAP)

a) Policy:-

- SISBL would not establish any business relationship with anonymous or fictitious/benami entities.

- SISBL would not establish business relationship or close an existing business relationship where SISBL is unable to apply appropriate customer due diligence measures i.e. unable to verify the identity and/or obtain documents required as per SEBI/regularity authorities' circular/guidelines.

- SISBL would exercise due care before admitting new client so as to ensure that the identity of the client does not match with any person with known criminal background or banned entities.

- SISBL would keep the customer profile as confidential.

b) Risk Based Approach:-

In order to ensure efficient implementation of the AML framework by regularity authority, it is necessary to establish a risk-based process on the basis of business activity of the intermediary. It is recognized that a higher level of due diligence and monitoring would be specified for business areas prone to higher money laundering risk.

Accordingly, individuals and entities whose identities and sources of wealth can be easily identified may be categorized as low risk (example: customer with well defined salary structures).Further, customers that are likely to pose a higher than average risk to SISBL may be categorized as medium or high risk depending on factors such as customer's backgrounds, nature and location of activity etc. (example: clients in high risk countries i.e. where fraud is highly prevalent or sponsors of international terrorism like Dubai, Afghanistan etc., client of special category (CSC) or introduced by CSC).

SISBL has also have a process to check the list of Designated Individuals / Entities as per "UNSCR List" in accordance with the SEBI master circular on Anti- Money Laundering CIR/ISD/AML/3/2010 dated December 31, 2010 & communiqué 2236 and clause 5 of Part II of SEBI master circular CIR/MIRSD/1/2014 dated March 12, 2014 & communiqué 4309 before opening an account.

While following the KYC norm, we have already introduced the above mentioned process by taking PMLA declaration from the proposed constituent. The details of such declaration in the KYC form are as follows:

"PMLA DECLARATION

I/We further declare that the Policy on Prevention of Money Laundering Act. (PMLA) 2002, has been duly explained to me/us by the Trading Member and Depository Participant which is also available at https://fiuindia.gov.in and I/We have understood the contents there in. I/We further declare and confirm that I/We do/does not have any connection to any of the categories as mentioned below:

1) *any Current/Former Head of state, Current or former Senior High profile politicians and connected persons (immediately family, close advisors and companies in which such individuals have interest or significant influence);*

2) *any connection with any entity or group whose existence is deemed illegal as per the law of the land;*

3) *any connection with any entity or group who has been found guilty as per the provisions of the laws of the land;*

4) *any connection with any Politically Exposed Person (PEP) of foreign origin or his/her family member;*

5) *any connection with any Charities, NGOs and organizations receiving donations;*

6) *any connection with any Current/Former Head of state, Current or Former Senior High profile politicians and connected persons (immediately family, close advisors and companies in which such individuals have interest or significant influence);*

7) *any connection with any Countries reputed to be any of the following-Havens/sponsors of international terrorism, offshore financial centers, tax havens, Countries where fraud is highly prevalent;*

8) *any connection with any high risk countries where existence/effectiveness of money laundering control is suspect, where there is unusual banking secrecy;*

9) *any connection with any Companies having close family shareholdings or beneficial ownership.*

I/We hereby declare that I/We fall under Clients of Special Category as defined in Prevention of Money Laundering Act 2002 (choose the relevant Category as under) [ ] Non Resident Client [ ] High Net- orth Clients [ ] Trust, Charities, Non-Governmental Organisations (NGOs) and organizations receiving donations [ ] Companies having close family shareholdings or beneficial ownership [ ] Politically Exposed Persons [ ] Companies Offering foreign exchange offerings [ ] Clients in high risk countries where existence/ effectiveness of money laundering controls is suspect [ ] Non face to face clients [ ] Clients with dubious reputation as per public information available etc.

OTHER DECLARATION

I/We have been investing in Stock Market,	*[ ] No experience* *[ ] Less than 3 years* *[ ] Between 3 and 7 years* *[ ] More than 7 years*
Normally, I/ We invest in Stock Market,	*[ ] Less than 10%* *[ ] Between >10% and 25%* *[ ] Between >25% and 50%*
I/ We hereby declare that, I/ We can take loss,	*[ ] Less than 10%* *[] Between >10% to 20%* *[ ] Between >20% to 30%* *[ ] More than 30% of my/our investment in Stock Market.*
I/We hereby declare that, return expectation from the investment in any market condition is,	*[ ] Less than 10%* *[ ] Between >10% to 20%* *[ ] Between >20% to 30%* *[ ] More than 30%*
I/We intend to invest in Stock Market [ ] without any borrowed fund / [ ] with borrowed fund and which is,	*[ ] Less than 10%* *[ ] Between >10% to 30%* *[ ] Between >30% to 50%* *[ ] More than 50% of my/ our monthly income."*

3.6.2 Customer Identification Procedure (CIP):-

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source of documents, data or information. Operating staff should exercise due diligence and care while opening an account in terms of SEBI guidelines/regulations and legal compliance in force.

Due diligence will also involve correctly profiling the customer in the account opening forms covering the following:

- Client Category
- Occupation
- Date of Birth
- Marital status
- Introduction Details
- PAN
- Correspondence & Permanent address
- Bank a/c
- Demat a/c
- Income details etc.

At the time of opening the account we obtain the different types of proofs:

Identity and Address proof: Any one of Officially Valid Documents – OVD as stipulated by SEBI i.e. copy of proof of possession of Aadhaar number , Passport , Driving License , Voter's Identity Card issued by Election Commission of India .Apart from that Pan card to be submitted mandatorily.

List of documents for Deemed Proof of Address:

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill.) .
- Property of Municipal tax receipt.
- Persion or family persion payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings,if they contain the address.
- Letter of allotment accommodation from employer issude by State Government or Central Government Departments, statutory or regulatory bodies, publick sector undertakings, schedeled commercial banks, financial institution and listed

companies and leave and licence agreement with such employers allotting official accommodation.

Checking the genuineness of the PAN from "incometaxindiaefiling.gov.in/challan/enterpanforchallan.jsp" which is the authorized site of Income Tax Department, Govt of India

Taking the self signature of the client (with stamp in case of non individual clients) and also verify the photograph with the actual photo provided by the client.

In case of non individual client the PAN copy of the entity along with that of the authorized person(s) is also collected. The verification procedures should be same as above.

While collecting the identity proof for the purpose of opening account with us we follow the SEBI guidelines and it is also verified with original by our employee with signature & employee code. In addition to this, the proof should be self certified by client (with stamp in case of non individual clients).

While collecting the address proof for the purpose of opening account with us we follow the SEBI guidelines and it is also verified with original by our employee with signature & employee code. In addition to this the proof should be self certified by client (with stamp in case of non individual clients) for offline account opening and for online account opening we follow the process as per SEBI circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020.

- **Photograph:** The photograph affixed in the form should be of the identical person for whom in-person verification has been done.

- **Email & Mobile:** Incase of email we also send a mail to the declared email of the client for verification purpose and call to his/her declared mobile for reconfirmation and in case of mobile we are checking the mobile by calling the client directly.

Further, In cases where in the same mobile number/email address is captured in more than one demat account and the family flag is also not updated, SISBL shall issue 30 days notice to such demat account holders for submitting the mobile number/email address modification form/request letter for updating the same or family flag declaration or to provide the updated mobile number/email address for updating in the demat account. If such request is not received within stipulated time even after followup, such KYC would be classified as non-compliant accounts (due to invalid

mobile or email ID). Thereafter, such non-compliant demat accounts will be liable to be made inactive i.e., no debit will be allowed in such demat account".

SISBL will also ensure that the mobile numbers/email address of its employee is not updated in the Participants/ Clients account.

- **Income & occupation**: We collect and scrutiny the client income information, occupation (viz. salaried, businessman etc.) with the relevant proof (where applicable) as required under SEBI Regulation.

- **Miscellaneous measurements:** While opening the account we are taking some general checking points like, the client has any criminal back grounds, client has any connection with broking business.

- **Clients under NRI/Foreign National category:** In case of NRI client, we are collecting copy of passport along with copy of PAN card in addition to OCI and PIO details if applicable, PIS approval of NRE Account , FEMA and FATCA/CRS Declaration as applicable.

- **For Companies :** Copy of the balance sheets for the last 2 financial years ,Copy of latest share holding pattern including list of all those holding control, either directly or indirectly in the company in terms of SEBI takeover Regulations duly certified by the company secretary / Whole time directors / MD , Photograph POI POA PAN and DIN numbers of whole time directors / two directors in charge of day ro day operations, Photograph POI POA PAN of individual promoters holding control – either directly of indirectly, Copies of Memorandum and Articles of Association and Certificate of incorporation, Copy of Board Resolution for investment in securities market (Trading & Demat), Authorised signatories list with specimen signatures.
- **For Partnership Firm/LLP**: - Copy of the balance sheets for the last 2 financial years ,Certificate of registration (for registered partnership firms only), Copy partnership deed, Authorised signatories list with specimen signatures, Photograph POI POA PAN of Partners.
- **For Trusts and Foundations :-**Copy of balance sheets for the lat 2 financial years ,Certificate registration (for registered trust only), Copy trust deed List of trustees certified by managing trustees / CA, Photograph POI POA PAN of trustees.
- **For HUF:-** Pan of HUF, Deed of declaration of HUF / List of coparceners in the HUF along with an authorization given to the Karta by the said coparceners to open and operate the DP and Trading accounts, Bank pass-book / Bank statement in the name of HUF, Photograph, POI POA PAN of Karta.

Further, Additionally in case of client being a non-profit organisation SISBL ensures that the same is registered on the DARPAN Portal of NITI Aayog, and will collect such registration details at the time of account opening and maintain such registration records for a period

of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

The CDD process of non-profit organisation involves the following key steps:

Over and above the process of CDD followed for Non Individual entities the below mentione steps to be observed:

Mandatory Identity Verification (The NGO-DARPAN Factor)

Registration on NGO-DARPAN is generally a prerequisite for NPOs to receive government grants or foreign funding (FCRA) in India.

- DARPAN Unique ID: To obtain and verify the NPO's Unique ID issued by NITI Aayog.
- Portal Validation: Cross-check the registration status directly on the live NGO-DARPAN portal to verify the NPO's active status, sector of operation, and registered address.

The updation of documents during Client Due Diligence is classified into two groups. Such as

- **Individual clients:-** For Individual clients SISBL collects required documents, to resolve the query as revealed in the alert generated by us. SISBL also collect income proof from the clients who are trading in the derivatives segment as required by the regulation.
- **Non Individual clients:-** For Non Individual clients SISBL collects all the documents as required in the regulation.

SISBL do not rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.

SISBL exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds or securities.

SISBL determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner.

As per current Prevention of Money-laundering (Maintenance of Records) Amendment Rules, the beneficial owner means: -

- where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than Ten percent of shares or capital or profits or who exercises control through other means;

- where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/ entitlement to more than Ten percent of capital or profits of the partnership;

- where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than Ten percent of the property or capital or profits of such association or body of individuals;

- where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

- where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with Ten percent 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;

Process to identify and reporting for FATCA / CRS

FATCA (Foreign Account Tax Compliance Act):

Purpose:

FATCA aims to prevent US taxpayers from avoiding taxes by holding assets in offshore accounts.

Obligation:

RFI like SISBL are required to identify and report on accounts held by US citizens, residents, and certain entities.

Reporting:

SISBL report information to the KYC Registration Agency along with TIN for applicable clients for KYC validation and Form 61B, (also known as the Statement of Reportable Account), is a report to be furnished by a RFI regarding each account that has been identified as a reportable account to Income Tax Department, pursuant to the due diligence procedure specified in rule 114H.

CRS (Common Reporting Standard):

Purpose:

The Common Reporting Standard (CRS), worldwide standard for the automatic exchange of financial account information between participating countries.

Obligation:

RFI need to identify account holders who are tax residents of other participating countries and report their financial information to the relevant tax authorities.

Reporting:

SISBL report information to the KYC Registration Agency along with TIN for applicable clients for KYC validation and Form 61B, (also known as the Statement of Reportable Account), is a report to be furnished by a RFI regarding each account that has been identified as a reportable account to Income Tax Department, pursuant to the due diligence procedure specified in rule 114H.

SISBL Role:

Collection of Information:

SISBL collects information about clients' tax residency, including their status for FATCA and their residency in other participating countries for CRS.

Self-Certification:

Account-holders (both individual and entity) must declare their tax residence to determine the status (to be considered “Non-residents” or “Foreign National / “Foreign Entity”) via self-certification.

Reporting:

SISBL report information to the KYC Registration Agency along with TIN for applicable clients for KYC validation and Form 61B, (also known as the Statement of Reportable Account), is a report to be furnished by a RFI regarding each account that has been identified as a reportable account to Income Tax Department, pursuant to the due diligence procedure specified in rule 114H.

Compliance:

Clients need to be aware of these requirements and provide the necessary information to SISBL to ensure compliance.

How to Update FATCA/CRS Information:

Offline Process:

The process of updating FATCA/CRS information with SISBL is primarily offline. Clients need to contact Regional manager (RM), Branch In charge, or CRM for assistance.

Collection of Data through KYC Updation Form:

Clients will receive a KYC (Know Your Client) updation form, which includes the FATCA / CRS declaration and required to submit countries details along with Tax ID number.

Submission:

Clients has to submit the documents at the time of on boarding and can update their current status through signed scanned copy of FATCA / CRS declaration through email to helpdesh@shriraminsight.com or submit it to our nearest Branch or service center.

Verification Process:

After obtaining TIN or functional equivalent from the clients through FATCA / CRS declaration if applicable for respective counties, we are checking the clients Tax Identification number **"TIN structure Individuals and or TIN structure - Legal Entities"** from the file provided by CVLKRA.

Capturing of Data for Reporting purpose for Filling of Form 61B:

At the time of on boarding of clients, we are capturing all information related to FATCA and CRS in our Client Master (back office system) which we are populating at the time of generating the uploadable file for Form 61B.

To promote tax transparency, below is the key information of clients which are stored at our system for reporting purpose.

- Personal identification information, such as clients name, Indian address and /or foreign address.
- Client Identification number, Gender, Mobile number, Email id, date of birth, place of birth, country of birth, Currency in which account is maintained etc.
- End-of-calendar year balances and valuations of Demat holding

- Demat Account/ Trading Account Number.
- Account type, Account category, nationality, country of residence, occupation type etc.
- TIN or functional equivalent of the clients if applicable.

Risk Management Procedure to determine whether their client or potential client or the beneficial owner of such client is a Politically Exposed Person (PEP) and / or Client of Special Category (CSC)

- Determining the beneficial owner of such client who is a Politically Exposed Person (PEP) and / or Client of Special Category (CSC).
- Obtaining senior management approval for establishing business relationships with Politically Exposed Person (PEP) and / or Client of Special Category (CSC).
- Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, then also senior management approval required to continue the business relationship.
- To check and or understand source of fund.
- Client Identification process should be done by using reliable sources including documents / information.
- Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher Authorities.
- Minimum information/documents to be collected from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients irrespective of investment amount.

3.6.3 Transaction monitoring and reporting especially Suspicious Transactions Reporting(STR):-

SISBL maintain records of all suspicious transactions.' Suspicious transaction' 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;(b)appears to be made in circumstances of unusual of unjustified complexity, or (c) appears to have no economic rationale of bonafide purpose. The records pertaining to suspicious transaction

would contain the date on which the transaction was conducted, the nature of transaction, the amount of transaction & the party to transaction was executed.

a) **Nature of transaction:** At the time of identifying the suspicious transaction we consider the following transactions can be suspicious in nature:

i. Huge transactions not match with client's income & assets (like.demat holdings).
ii. Continuous payment made by demand drafts/pay order/banker's cheque etc. or bouncing of cheques including any stocks or fund received from any entity other than client.
iii. Huge or continuous off market transactions.
iv. Unusual rise in transaction volume without any justified economic reason.
v. Unusual huge transactions done immediately after activation in a code which was dormant.

SISBL keeps the stocks and fund received from any entity other then clients separately and do not allow it to move into the market, in addition to that any stocks and funds is also getting feezed by us if as per the advice given by any Regulators, Income Tax authority, Police Authority etc

The above transactions are illustrative only. SISBL review & update it time to time.

b) **Parties to transactions:** For the purpose of identifying the suspicious transactions the following clients of special categories(CSC) are taken into account:

i. High Net worth Client.
ii. Nonresident in India.
iii. Politically Exposed Person (PEP) of foreign origin or his/her family member.
iv. Client with Criminal offence or his/her family member.
v. Companies having close family shareholdings.
vi. Trust, Charities, NGOs and organizations receiving donations.
vii. Current/Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, close advisors and companies in which such individuals have interest or significant influence).
viii. Companies offering foreign exchange offerings.

Process of Identifying & Monitoring of Suspicious Transactions:

I. Identification process of Suspicious Transactions:

A transaction can be identified as suspicious from the following way from documents departments report:

i. Daily turnover report (which include synchronized/high volume/square up trades).
ii. Fortnightly demat transaction report.
iii. Weekly High value cheque bounces report.
iv. Weekly High value DD/PO/Banker's cheque payment report and
v. Monthly turnover report.

Intimation of CSC client registration should be given to A/Cs, Delivery, DP (for DP client) & Risk department by Documents department so that all transactions of this client can be monitored since beginning.

II. Monitoring of Suspicious Transactions:

All this report of suspicious transactions will go to Head of A/Cs, Delivery, DP, Risk, and Internal Audit & Compliance department for their perusal. One copy of this report should reach to Principal Officer within the next 2 working day.

Designated department will conduct exhaustive checking of KYC and annexed documents of all suspicious clients as well as CSC clients within next working day. Similarly A/Cs, Delivery, DP & Risk department will also give report to Principal Officer regarding whether they have noticed any irregularities in transactions done by CSC and these suspicious clients will be rescruitinised by concerned department. Contract notes, share ledger, funds ledger & other audit trials of transactions will also be checked on a sample basis and report will be given to Mr. Partha Pratim Hazra (CEO & Designated Director), Mr.Manas Roy Choudhury (COO & Designated Director), Mrs.Chandana Dutt (CFO) who will in turn have a meeting with the Principal Officer. Any serious issue is to be highlighted to the Principal Officer immediately.

On the basis of these reports necessary action is taken by Principal Officer including filing of suspicious report. Necessary steps will also be initiated for closure of account, if required. A report containing all transaction exceeding Rs. 10 lacs should come to Principal Officer for his scrutiny. No Bank Draft/PO/Bankers Cheque will be accepted from CSC as it will have no audit trial of customer's source of fund like A/C payee cheque.

If it is found that transactions of any clients has increased rapidly in a very short span of time which is not commensurate with his financial conditions as disclosed in the KYC of the client then special care should be taken to scrutiny this accounts & ask for further requirements like latest financial status etc. Moreover no client will be allowed to trade without sufficient Margin.

In case of dormant account of twelve months, before activation of such account we review the client registration documents in the light of recent circular given by regularities and as

well as call/contract to client to confirm the genuineness before activation under the same UCC if so required.

III) Transaction for DP:

Irrespective of market/off market transaction, if the value of transaction exceeding Rs. 10 lacs we are getting confirmation from the client. Moreover this transaction is scrutinised by the senior official only. Incase of dormant account, if there is any high value transaction has taken place before approving the transaction we are checking the authenticity of the transaction by cross checking the client.

IV. Retention of Records:

SISBL shall maintain appropriate documentation like KYC, Agreement, DI slip, Contract Note etc. filed in account no. wise & date wise and are kept in separate godown with proper store records. It is retained and supervised by senior official of the company. The records shall be maintained for a period of five years (Eight years in terms of Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 for Depository Participants) from the date of cessation of the transaction. Records shall be maintained in a manner, which facilitates its easy retrieval as when required. However, in situations where the records are subject to on-going investigations or prosecution in court, SISBL shall retain such records beyond the stipulated retention period until it is confirmed by the Financial Intelligence Unit/by appropriate authority, that such records are no longer needed.

3.7 Combating Financing of Terrorism:-

In terms of PML Rules, suspicious transaction should include, inter alia transactions which give rise to a reasonable ground of suspicion that it may involve the proceeds of an offence mentioned in the Schedule to the PMLA, regardless of the proceeds of an offence mentioned in the Schedule to the PMLA, regardless of the value involved.

SISBL has developed suitable mechanism through appropriate policy framework for enhanced monitoring of transactions suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit-India (FIU-IND) on priority.
While CDD, SISBL checks the list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) received form Govt. of India and circulated by the Regulators. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in

splitting of the 1267 Committee's Consolidated List into two separate lists, namely -

- https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

LIST OF DESIGNATED INDIVIDUALS / ENTITIES AND FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

- We have system in place to ensure that no client is registered with us whose name is appearing in the list of individuals & 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).

The list is accessed in the UN website at

- https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

- We have system in place to 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 are required to be intimated to SEBI and FIU-IND.

- SISBL shall run a check 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.

- In the event, particulars of any of customer/s match the particulars of designated individuals/entities, SISBL shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets etc held in the form of securities, held by such customer on their books 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.

- SISBL shall send particulars of the communication mentioned above, through post 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.

- In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, SISBL shall 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.

3.8 Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries

- The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.
- In terms of Section 12A of the WMD Act, the Central Government is empowered as under:
  "(2) For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

  (a) Freeze, seize or attach funds or other financial assets or economic resources—

  - owned or controlled, wholly or jointly, directly or indirectly, by such person; or
  - held by or on behalf of, or at the direction of, such person; or
  - derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

  (b) prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant

Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

- The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."
  The stock exchanges and registered intermediaries are directed to comply with the procedure laid down in the said Order.
- The stock exchanges and registered intermediaries shall:
  Maintain the list of individuals/entities ("Designated List") and update it, without delay, in terms of paragraph 2.1 of the Order;

  Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), without delay. The details of the CNO are:- The Director, FIU – INDIA, Tel.No - 011-23314458,Email - dir@fiuindia.gov.in.

4 Internal Controls and Structures of SISBL:-

4.1 Empanelment of Designated Director with FIU-IND:-

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. SISBL nominate **Mr. Partha Pratim Hazra** its Board as "Designated Director", as per the provisions of the PML (Maintenance of Records) Amendment Rules, 2013. The name, designation and address of the Designated Director are to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

4.2 Principal Officer:-

SISBL designated Mr. Gautam Sarkar as Principal Officer as per the provisions of the PML (Maintenance of Records) Amendment Rules, 2013. The name, designation and address of the Designated Director are to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND)

SISBL has also designated Mr.Manas Roy Choudhury, Mrs.Chandana Dutt , Mr. Souvik Ghosh for periodical review of the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. If any change in regulation or introduction of new circulars has an impact on the policy, then only the modification being done to the policy and a new version is getting updated.

4.3 Reporting Obligation under PMLA .

In terms of the Rules notified under Prevention of Money Laundering Act (PMLA), 2002, Suspicious Transaction Reporting (STR) is the obligation casted on Stock Brokers with regard to reporting.

Suspicious Transaction Reporting (STR):-

As per PMLA Rule 2(g) Suspicious Transaction means a transaction whether or not made in cash which to a person acting in good faith –

- gives rise to reasonable ground of suspicion that it may involve the proceeds of crime or
- appears to be made in circumstances of unusual or unjustified complexity or
- appears to have no economic rationale or bonafide purpose gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism .

Generation of Alerts:-

Alert generation involves application of scenarios and risk factor to detect potentially suspicious activity. Effective alert generation is very critical to the quantity and quality of the STRs generated by Brokers. Indicators are circumstances that indicate suspicious nature of transactions. Suspicious transaction may be detected from one indicator or a set of indicators.

SISBL has adequate processes and systems for detection of transactions and reporting of suspicious transactions, identified by the employee and are using centralized Alert Generation Software recommended parameters in the act.

4.4 Identification of Suspicious transactions by SISBL:-

The identification of suspicious transaction by SISBL is more likely to be related with the following sources:

- **Transaction Monitoring (TM):** Transaction monitoring alert (e.g. unusually large transaction, increase in transaction volumes etc.)

- **Watch List (WL):** The customer details matched with watched with watch lists (e.g. UN list, TF etc.)

- **Risk Management System (RM**): Risk Management system based alert (e.g. high risk customer, country, location, source of funds, transaction type etc.)

- **Customer Verification (CV):** Detected during customer acceptance, identification or verification (excluding reasons mentioned on other codes e.g. use of forged ID, wrong address etc.)

- **Law Enforcement Agency Query (LQ):** Query or letter received from Law Enforcement Agency (LEA) or Intelligence Agency (blocking order received, transaction details sought etc.)

- **Employee Initiated (EI**): Employee raised alert (e.g. behavioural indicators such as customer had no information about transaction, attempted transaction etc.)

- **Public Complaint (PC):** Complaint received from public (e.g. abuse of account for committing fraud etc.)

- **Business Associates (BA):** Information received from other institutions, subsidiaries or business associates (e.g. cross-border referral, alert raised by agent etc.)

- **Media Reports (MR):** Adverse Media Reports about customer (e.g. news paper reports)

The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, is of suspicious nature.

4.5 Filing of Reports to FIU-IND:-

The Prevention of Money Laundering Act (PMLA) and the rules there under require every financial institution to furnish to FIU-IND the statutory reports i.e. CTR, STR, CCR, NTR and CWTR within time schedule. In January 2022 FINGate 2.0 Portal was launched by FIU -IND . As part of the envisaged FINnet 2.0 system all Reporting Entities (REs) registered in FINnet 1.0 were mandatorily required to reregister themselves in FINnet 2.0 module. As per the reregistration exercise REs were required not only required to register their Principal Officer but the details of the Designated Director was also needed to be provided. FIU also did away with the earlier XML file format as well as the Report Generation Utility and Report Validation Utility used for filing Reports to FIU-IND. It introduced three reporting mechanisms in the newly launched FINnet 2.0. These mechanisms are as follows:

- Mechanism 1: Interactive web-based reporting
- Mechanism 2: Bulk report preparation app
- Mechanism 3: API based reporting

The Interactive web-based reporting mechanism is user friendly, context sensitive which consists of web-based forms. The forms have built-in form and field level validations. As FIU recommends this mechanism for Reporting Entities that have low volume reporting we are currently using only this mechanism for filing STRs.

4.6 Employees Screening & training:-

Identity & Address Verification

The first step in conducting a thorough Background Check is to verify that the applicant is providing accurate and honest information about their identity and address. From time to time applicants may conceal their previous addresses held in an attempt to hide prior criminal convictions or records.

Education Verification

With every one in four candidates reportedly falsifying education records, this check has become a standard procedure of a sound background screening program. Here we verify candidate's educational background. Education Verification includes verification of certificates of:

- Qualification obtained (Degree)
- University, Institute, College or School
- Year of Passing or Graduation
- Grade / Marks / Class
- Coursework or Specialization etc.

To assure the integrity of the data, we contact the Registrar / Controller of Examination of the schools, universities, and colleges to verify, if needed.

Employment Verification

Often prospective candidates make false claims or inflate information pertaining to their previous employment in order to get better position and higher salary. With the employment check we ensure that the information provided by the candidate regarding their work

experience is accurate and legitimate. Here we also check if there were any integrity related issues during the tenure at each employment held.

Employment verification includes verification of:

- Employer
- Dates of Employment
- Designation held
- Last Salary Drawn (CTC)
- Reasons for Leaving
- Breach of Contract
- Additional comments such as: Integrity, Known conflicts at workplace, violations, etc.
- Eligibility to Re-hire

Criminal Background Check

Criminal Records Checks in India essentially involves obtaining local criminal record information equivalent to Country Court records checks in the US. The checks are carried out at the local or central police departments having jurisdiction over the applicant's residential address.

Reference Check

A Reference Check is typically accompanied with the previous employment check. While employment verification aims to verify the objective facts about the employment from the HR department, the purpose of a supervisor reference check is to get further insight into the applicant's performance, capabilities and areas of improvement.

Integrity Check

Here a customized search is undertaken by team to assess candidate's behavior pattern, history and background. Integrity check is ideal for senior level hires. It's absolutely essential given the risks faced by enterprises today.

4.7 Employee Training:

Adequate ongoing program shall be conducted for all employees of front office staff, back office staff, compliance staff, risk management staff and staff dealing with new customers.

The AML training program shall address the requirements relating to the following:

- Meaning of money laundering.

- Identification of suspicious transactions.
- AML requirements.
- Possible risk of not adhering to the AML requirements.
- Requirements for adequate AML procedures.
- Methods of recognition of suspicious transactions or suspicious behavior of a client.
- Reporting system of suspicious transactions.

Training is related to employees' daily work and any updation in the rules and regulation. Important policies are communicated on a periodic basis among the employees.

Tipping off:

Generally no restriction is made on operations in the accounts where an STR has been made unless it is something extraordinary. Company and Our Directors, Officers and Employees are strictly prohibited from disclosing (tipping off) the fact that a STR or related information is being reported or provided to the FIU-IND. The prohibition of Tipping Off extends not only to the filling of the STR and/or related information but even before, during and after the submission of an STR. Thus, it is insured that there is no Tipping Off to the client at any level.

Customer Education:

SISBL shall educate the clients on the objectives of KYC/AML relate programme of the intermediary by the following way:

- Preparation of specific literature/pamphlets.
- Hosting relevant KYC/AML information on the website of SISBL.

5 Preservation of Records.

5.1 Purpose of maintaining records

The keeping of proper records is essential to enable SISBL to demonstrate that it has operated in conformity with local laws and regulations. This will in turn enable SISBL and individual staff members to defend themselves against any allegations of knowingly assisting a money launderer. SISBL must retain records concerning customer identifications as evidence of the work they have undertaken in complying with their legal and regulatory obligations as well as for use as evidence in any investigation conducted by law enforcement.

SISBL maintain records of the identity of the clients and records of transactions in hard and soft format. Rule 10(2) refers the records of the identity of clients shall be

maintained in a manner as may be specified by its regulators from time to time. Regulator has to specify the procedure and manner of maintaining the records of the identity of the clients.

5.2 Records to be preserved

To satisfy the requirements of investigation, the following documents to be preserved:

a) the origin of the funds funds and securities (if known);

b) nature of transactions;

c) the amount of transactions;

d) the date on which the transaction was conducted;

f) the identity of the person undertaking the transaction;

g) the parties to the transaction;

h) the destination of the funds and securities;

Records of the identity of clients shall include records of the identification data, account files and business correspondence etc.

The Company shall also maintain a record of all the transactions for a period of five years (Eight years in terms of Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018 for Depository Participants, from the date of the transaction with the Clients, which include:

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

b. all series of cash transactions integrally connected to each other, which have been individually valued below Rs. 10 Lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month and the monthly aggregate exceeds an amount of Rs.10 Lakhs or its equivalent in foreign currency.

c. all suspicious transactions whether or not made in cash and by way of credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by us.

5.3 Period of retention of records

As per the PMLA, the account opening records including identification documents should be kept for 5 years from the date of cessation of the transactions/relationship between the customer and SISBL and transaction records including Delivery Instruction slips, other forms of Records relating to investigations and transactions, which have been the subject of a disclosure, should be kept for 5 years from the time the STR is filed with FIU-IND. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also regulatory authorities. The term 'cessation' would broadly mean the time of closure of account. But there should have some exceptions:

a) In the matter related to a suspicious transaction is pending in a court, the relevant record should retained for 10 years from the date of final verdict of the court.

c) In specific cases, where SEBI/FIU-IND or any other regulatory body requests for the retention of records for a period more than 5 years , the bank should be guided by such specific request.

5.4 Indicative Alert Indicators :-

Sl. No.	Alert Indicator	Indicative Rule/Scenario
1	Customer offered false of forged identification document.	Customer given false identification documents or documents that appears to be counterfeited, altered or inaccurate.
2	Identity documents are not verifiable	Identity documents presented are not verifiable i.e. Foreign documents etc.
3	Address found to be non existent	Address provided by the customer is found to be nonexistent.
4	Address found to be wrong	Customer not staying at address provided during account opening.

5	Difficult to Identify beneficial owner.	Customer uses complex legal structures or where it is difficult to identify the beneficial owner.
6	Customer is being investigated for criminal offences.	Customer has been the subject to inquiry from any law enforcement agency relating to criminal offences.
7	Customer is being investigated for TF offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities.
8	Adverse media report about criminal activities of customer	Match of customer details with persons reported in local media/open source for criminal offences.
9	Adverse media report about TF or terrorist activities of customer.	Match of customer details with persons reported in local media/open source for terrorism or terrorist financing related activities.
10	Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal. Possibly false or inconsistent.
11	Customer avoiding nearer branches	Customer travels unexplained distances to conduct transactions.
12	Customer wants to avoid reporting	Customer makes inquiries tries to convince staff to avoid reporting.
13	Customer could not explain source of funds or securities.	Customer could not explain source of funds or securities satisfactorily.

24	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
15	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.
16	Complaint received from public.	Complaint received from public for abuse of account for committing fraud etc.
17	Alert raised by Authorised Person	Alert raised by Authorised Person about suspicion
18	Sudden high value transaction for the client	Sudden high value transaction for the client
19.	High value transactions in a new account	Transactions greater than INR[10 Lac] in newly opened.
20.	High value transactions in a dormant account	Transactions greater than INR [10 lac] in dormant account.
21.	Funds and Stocks received from unidentified account.	Any fund or securities received from third party account (not registered with SISBL as an investor) are kept in a separate account.