Arya Fin-Trade (IFSC) Private Limited

& Other Group Entities Registered Under IFSCA

Policy & Procedures for Prevention of Money Laundering (ML), Terrorist Financing (TF) & Know You Customer (KYC).

(Anti - Money Laundering Policy & Procedures)

APPLICABILITY: Guidelines of International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 shall apply to Arya Fin-Trade (IFSC) Private Limited and other entities of Arya Group which have regulated licensed Unit in IFSCA.

The guidelines and this policy are governed by Prevention of Money-laundering Act, 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, respectively.

POLICY & PROCEDURES COVERS

- Money Laundering Risk (ML Risk)
- Terrorist Financing Risk (TF Risk)
- Customer Due Diligence (CDD)
- Customer Acceptance & Identification Procedure
- Digital Kyc (E-KYC)
- Risk Categorization
- Risk Management
- Alert Generation (AML Alert)
- Transaction Monitoring
- Suspicious Transaction Reporting (STR)
- Record Keeping
- Freezing & Unfreezing Of Financial Assets
- Employee Hiring & Training
- Investor Education

Objectives

At National Level

To begin with, the Indian Government introduced the Prevention of Money Laundering Act, 2002, and corresponding regulations in a dedicated effort to prevent money laundering.

PMLA aims to prevent money laundering and provides for stringent penal consequences, including confiscation of property, when the transaction or the person is identified as associated with or involved in money laundering.

PMLA and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, lay down stringent regulations for the identified regulated entities, directing them to implement measures like thorough customer identification, reporting any suspicious transactions, maintaining AML records, etc.

At IFSC Level

Following the PMLA and the overall FATF Recommendations, the IFSCA issued the IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.

These IFSCA (AML, CTF, & KYC) Guidelines elaborate on the methods the IFSCA-regulated entities must adopt to identify the risk associated with money laundering and terrorism financing and deploy adequate risk mitigation measures, such as Customer Due Diligence and training the team. At IFSC

What is Money Laundering?

Money Laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. Through money laundering, the launderer transforms the monetary proceeds derived from criminal activity into funds with an apparent legal source.

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.

The term “Money Laundering” is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime).Money Laundering is a process of making dirty money look clean.

Money is moved around the financial system again and again in such manner that its origin gets hidden

1.5 Need for Anti Money Laundering:

It has become more evident that the next generation of identity thieves will deploy sophisticated fraud automation tools

The increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal money can be laundered

Every year, huge amounts of funds are generated from illegal activities. These funds are mostly in the form of cash

The criminals who generate these funds try to bring them into the legitimate financial system Over $1.5 trillion of illegal funds are laundered each year

Successful money laundering activity spawning yet more crime, exists at a scale that can and does have a distorting and disruptive effect on economies, marketplaces, the integrity of jurisdictions, market forces, democracies etc.

The IFSCA AML/CFT Guidelines emphasize the need for anti-money laundering efforts to:

a. Protect the integrity of financial systems.
a. Prevent financial institutions from being used to launder money.
b. Mitigate risks to the global and Indian financial systems by adhering to **FATF** and **UNSC** sanctions.

1.6 Consequences of Money Laundering

1.6.1 Finances Terrorism:

Money laundering provides terrorists with funds to carry out their activities

1.6.2 Undermines rule of law and governance:

Rule of Law is a precondition for economic development – Clear and certain rules applicable for all.

1.6.3 Affects macro economy:

Money launderers put money into unproductive assets to avoid detection.

1.6.4 Affects the integrity of the financial system:

Financial system advancing criminal purposes undermines the function and integrity of the financial system

1.6.5 Reduces Revenue and Control:

Money laundering diminishes government tax revenue and weakens government control over the economy.

1.7 Stages of Money Laundering

Although money laundering is a complex process, it generally follows three stages:

- Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring—breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.
- Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.
- Integration is the final stage in the re-injection of the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds. Banks and financial intermediaries are vulnerable from the Money Laundering point of view since criminal proceeds can enter banks in the form of large cash deposits.

1.8 FINANCIAL INTELLIGENCE UNIT (FIU) INDIA

The Government of India has set up the Financial Intelligence Unit (FIU-India) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

FIU –India has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspicious financial transactions. FIU India is also responsible for coordination and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

All regulated entities licensed with IFSCA are mandatorily required to register with the Financial Intelligence Unit of India (FIU-IND) by completing the enrolment on the FINGate 2.0 Portal.

The registration process involves furnishing the details about the business, the Principal Officer, and the regulated entity's Designated Director, who shall take care of the AML program within the organization.
The regulated entities under IFSCA must report any suspicious transactions or activities to FIU-IND.

b) KYC Standards

The objective of the KYC guidelines is to prevent Regulated entities from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable regulated entities to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

The KYC policy of the regulated entities incorporates the following four elements:

i. Customer Acceptance Policy (CAP)
ii. Customer Identification Procedures (CIP)
iii. Monitoring of Transactions; and iv. Risk Management

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

- A person or entity that maintains an account and/or has a business relationship with the regulated entities.
- One on whose behalf the account is maintained (i.e., the beneficial owner)
- Any person or entity connected with a trading transaction or any other financial transactions which can pose significant reputational or other risks to the regulated entities.

2.1 CUSTOMER ACCEPTANCE POLICY (CAP)

a) The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed.

The regulated entities shall accept customer strictly in accordance with the said policy and independent verification of each client must be done:

i. No account shall be opened in anonymous or fictitious/benami name(s)

ii. Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, product, service, transaction or delivery channel risk factors social and financial status etc., to enable categorization of customers into low, medium and high risk called Level I, Level II and Level III respectively; Customers requiring very high level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as Level III

iii. The Regulated entity shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by IFSCA from time to time

iv. The regulated entity shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., regulated entity is unable to verify the identity and/or obtain documents required as per the risk categorization due to noncooperation of the customer or non- reliability of

data/information furnished to the Regulated Entity. The Regulated Entity shall, however, ensure that these measures do not lead to the harassment of the customer. Further, the customer should be given a prior notice of at least 30 days wherein reasons for closure of his account should also be mentioned.

vi. The Regulated Entity shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.IFSCA has been circulating lists of terrorist entities notified by the Government of India or UNO so that the regulated entity may exercise caution against any transaction detected with such entities.
The Regulated Entity shall invariably consult such lists to ensure that prospective person/s or organizations, desirous to establish relationship, are not in any way involved in any unlawful activity and that they do not appear in such lists.

b) The Regulated Entity shall prepare a profile for each new customer based on risk categorization.

The nature and extent of due diligence shall depend on the risk perceived by the Regulated Entity. The KYC Staff should continue to strictly follow the instruction regarding secrecy of customer information. KYC Staff should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of services to the general public, especially to those, who are financially or socially disadvantaged.

c) The risk assessment requires a Regulated Entity to allocate an appropriate risk rating to every customer.

The risk ratings should be descriptive, such as “low”, “medium” or “high”. The outcome of the ML/TF risk assessment decides the degree of Customer Due Diligence that needs to be performed.

For a high-risk customer, the Regulated Entity shall undertake Enhanced CDD measures in addition to the normal CDD.

For a low-risk customer, the Regulated Entity may undertake Simplified CDD. For any other customer.

The Regulated Entity may undertake the normal CDD.

The risk to the clients may be assigned on the following basis:-

Sr. No	Risk Level	Description	Illustrative List
I	Low Risk	Individuals (excluding High Net Worth) and entities whose identities and sources of wealth are easily identifiable, and transactions in their accounts largely conform to known profiles are categorized as low risk.	Examples of low-risk customers include salaried employees with well-defined salary structures, individuals from lower economic strata with small account balances and low turnover, government departments, government-owned companies, regulators, and statutory bodies. Basic identity and location verification requirements must be met.
II	Medium Risk	Customers who are likely to pose a higher than average risk to the regulated entity are categorized as medium or high risk, depending on their background, nature and location of activity, country of origin, sources of funds, and their client profile.	Examples of medium- risk customers include individuals engaged in business/industry or trading activity in areas with a history of unlawful trading/business activity and those whose client profiles are uncertain and/or doubtful/dubious, as perceived by the Regulated Entity.
III	High Risk	The Regulated Entity may apply enhanced due diligence measures based on the risk assessment, requiring intensive 'due diligence' for higher-risk customers, especially those for whom the sources of funds are unclear.	Examples of High Risk Customers include Politically Exposed Persons (PEPs), Non- resident customers, and Cash-intensive businesses.

(d) Clients of special category (CSC)

Apart from above, there are clients of special categories which may include the following:-

a. Nonresident clients

b. High net worth clients, (High Net worth clients (i.e the clients having Net worth exceeding 5 Crore (or its equivalent in foreign currency) and doing the intraday trading volume of more than 7 Crore (or its equivalent in foreign currency) and daily delivery volume more than Rs 5 Crore (or its equivalent in foreign currency) and in case of DP; Holding stock of more than 5 Crore(or its equivalent in foreign currency))

c. Trust, Charities, NGOs and organizations receiving donations
d. Companies having close family shareholdings or beneficial ownership
e. Politically exposed persons (PEP) of foreign origin
f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
g. Companies offering foreign exchange offerings
h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
i. Non face to face clients
j. Clients with dubious reputation as per public information available etc. (dubious reputation means client having name in CIBIL, watchoutinvestor.com, defaulter list, etc.)

The above mentioned list is only illustrative and the Staff along with senior officials should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

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

Periodicity of updating documents taken during the client due diligence (CDD) process :

The periodicity of updating documents taken during the client due diligence (CDD) process is an important aspect of maintaining the integrity and accuracy of client information

1. Inactive Clients: For clients who have not engaged in any transactions for the past 2 years, documents taken during the CDD process must be updated at the time of reactivation. This ensures that the client's information is current and accurate before any new transactions are initiated.

2. Active Clients: For clients who are currently active, documents are updated on an annual basis if there have been any changes to their details. This includes any updates to personal information such as address, phone number, or employment status, as well as any changes to their financial information.

3. Oral Confirmation: In cases where there have been no changes to the client's information, an oral confirmation can be obtained from the client regarding the lack of change. This can be done in a phone call or during an in-person meeting, and should be documented for record-keeping purposes.

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

We may 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.

Provided such third parties shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

ii. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by IFSCA from time to time.

We shall be ultimately responsible even though we rely on third parties for the CDD Process.

2.2 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

a) Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information.

b) The Regulated Entity need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of broking relationship. Being satisfied means that the Regulated Entity is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.)

c) For customers that are natural persons, the Regulated Entity shall obtain sufficient identification data to verify the identity of the customer, his address/location, in person verification and also his recent photograph.

d) For customers that are legal persons or entities, the Regulated Entity shall

(i) Verify the legal status of the legal person/entity through proper and relevant documents
(ii) Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person
(iii) Understand the ownership and control structure of the customer and determine

- ♣ who are the natural persons,
- ♣ who ultimately control the legal person

e) If the Regulated Entity decides to accept such accounts in terms of the Customer Acceptance Policy, the Regulated Entity shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

Further,in terms of PMLA regulations and IFSCA guidelines for identification of Beneficial Ownership following procedures shall be adhered while opening account of non-individual clients.

<table>
<tr><td rowspan="4">Category of Client</td><td rowspan="4">Client Type</td><td colspan="3">Identification of Natural persons who have a controlling ownership interest</td></tr>
<tr><td>1</td><td>2</td><td>3</td></tr>
<tr><td rowspan="2">Basis of Identification</td><td>In case where there exist doubt under above identification point 1</td><td>If no person is identified under above identification point 1 & 2</td></tr>
<tr><td>Basis of Identification</td><td>Basis of Identification</td></tr>
<tr><td rowspan="3">Clients other than Individuals or Trusts (i.e., Company, Partnership or Unincorporated Association/Body of Individuals)</td><td>Corporate/ Company</td><td>Ownership/Entitlement of more than 10% of Shares or Capital or Profits</td><td rowspan="3">Control through means such as Voting Rights, Agreements, Arrangements, or any other manner</td><td rowspan="3">Relevant natural person who holds the position of senior managing official</td></tr>
<tr><td>Partnership Firm</td><td>Ownership/Entitlement of more than 10% of Capital or Profits</td></tr>
<tr><td>Unincorporated Association or Body of Individual</td><td>Ownership/Entitlement of more than 15% of Property or Capital or Profits</td></tr>
</table>

Exemption in case of Listed Companies	Identification and verification of shareholders or beneficial owners of listed companies is not required.		
Foreign Investors	(Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors)	List of beneficial owners with shareholding or beneficial interest in the client equal to or above 25% to be obtained.	Due diligence as per PMLA and IFSCA guidelines on AML about the financial position of the Foreign Investors may be carried out but is not mandatory. Intermediaries may take an undertaking from Global Custodian/Local Custodian to submit the list of beneficial owners. Any changes in the list should be obtained based on the risk profile of the client.

*In case of client being a **non-profit organization**, Regulated Entity shall get them registered on the DARPAN Portal of NITI Aayog, if not already registered, 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 late.*

Where Regulated Entity is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU IND.

2.3 OFFICIALLY VALID DOCUMENTS (OVDS) – VIS-À-VIS DIGITAL KYC

i. Verification of Identity of Customer

(a) A Regulated Entity shall verify the identity of the customer using reliable, independent source data,documents or information. Where the customer is a legal person or legal arrangement, a Regulated Entity shall verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.

(b) When relying on documents, a Regulated Entity should be aware that the most reliable documents to verify the identity of the customer are those which are most difficult to obtain illegally or to counterfeit. These may include government-issued identity cards or current valid passport, reports from independent company registries, published or audited annual reports and other reliable sources of information. The rigor of the verification process should be commensurate with the customer's risk profile.

(c) In verifying the identity of a customer, a Regulated Entity may obtain the following documents:

In case of Natural Persons –

(i) any of the OVD specified under these Guidelines that contains photograph of the customer, name, unique identification number, date of birth and nationality; and

(ii) residential address based on OVD or recent utility bill, bank statement or such other documents specified under the definition of OVD.

In case of Legal persons or Legal Arrangements-

Name, legal form, proof of existence and constitution: - the verification for the same can be obtained from certificate of incorporation, certificate of good standing, partnership deed/agreement, rust deed, constitutional document, certificate of registration or any other document from a reliable independent source.

Powers that regulate and bind the legal person or legal arrangement: - This can be ascertained from the constitutional documents, as well as the names of the relevant persons having a Senior Management position in the legal person or legal arrangement and board resolution or similar document authorising the opening of an account and appointment of its authorised signatories

In cases where a customer is a foreign national

In cases where a customer is a foreign national, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth and address of a foreign national would also be considered as OVD. In case where the customer is an Indian national, OVD shall include the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card, etc. as prescribed under the Rules (For more detailed understanding, refer OVD definition). For the purpose of customer verification,equivalent e-documents of OVDs shall also be treated as original document by a Regulated Entity.

In case of "equivalent e-document

In terms of PML Rule 2 (1) (cb) "equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the

investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

iv. In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) "Officially Valid Documents" means the following:
a. thepassport,
b. the driving licence,
c. proof of possession of Aadhaar number,
d. the Voter's Identity Card issued by Election Commission of India,
e. job card issued by NREGA duly signed by an officer of the State Government and
f. the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator

v. Further, Rule 9(18) of PML Rules states that in case OVD furnished by the investor does not contain updated address, the document as prescribed therein viz e.g. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)Or Property etc., shall be deemed to be the OVD for the limited purpose of proof of address, provided that the client shall submit updated officially valid document or their equivalent e-documents thereof with current address within a period of three months of submitting the above documents.

vi. PML Rules allows an investor to submit other OVD instead of PAN in case of Indian National however, In case of Indian National, the customer's PAN details, if available with the Regulated Entity, is verified from the database of the issuing authority at the time of periodic updation of CDD.

2.4 RISK BASED APPROACH (RBA) RISK MANAGEMENT

RISK BASED APPROACH (RBA)

Under a risk-based approach, a regulated entity's primary task is to identify and understand the source or factors emitting the risks and tailor the controls and overall AML program commensurate with the ML/FT risk assessed.
Regulated Entity is exposed, depending upon its nature of business and exposure to or involvement with certain types of clients, countries or geographic areas, products, services, transactions, or delivery channels, etc. and document the same. A Regulated Entity while adopting RBA shall ensure that:
(i) The RBA is objective and proportionate to the risks;

(ii) The RBA is based on reasonable grounds; and
(iii) The RBA is reviewed and updated at appropriate intervals.

Based on the risk assessment, the Regulated Entity shall monitor, manage, and mitigate the risks it is exposed to by applying effective, appropriate and proportionate measures.

Here comes the need to conduct the Enterprise-Wide Risk Assessment (EWRA) to evaluate and assess the money laundering and financing of terrorism risks associated with the entity's operations, business model, etc.

The Risk Factors

The risk may arise from various factors contributing to the business. Thus, the regulated must assess the potential ML/FT risks posed by various risk parameters such as:

- The nature and overall profile of the customer the regulated entity engages with
- The jurisdictions of the regulated entity's customers
- The nature of the products and services offered by the regulated entity
- Size and the complexity of the financial transactions
- Delivery or the distribution channels deployed, etc.
- Risks posed by the development of new product, practices, and technologies

ML/FT Enterprise-Wide Risk Assessment

Identification of the Risk

Identify the ML/FT risk the business is exposed to considering the following risk parameters-

- Type of customer & their business activities
- Geographies of business engagement
- Products and Services offered
- Delivery channels involved
- Transactions – volume and complexity
- Development of new product, practices and technologies

Analysis of Risk

Determining the probability of occurrence of risk and its resulting impact on the business

Once the relevant risk factors have been identified, the regulated entity must evaluate the possibility of such risk occurring and its impact on the business.
This analysis will help the regulated entity determine the level and nature of risk mitigation measures (controls and systems) required to handle these risks.

Thus, after assessing the risk and the required measures, the regulated entity must outline a larger ML/FT risk management and compliance0020framework.

2 Customer Risk Assessment & Anti-Money Laundering – KYC Standards

a) Customer Risk Assessment

A Regulated Entity shall

i. undertake a risk-based assessment of every customer; and

ii. assign the customer a risk rating proportionate to the ML/TF risks

The customer risk assessment shall be completed prior to undertaking Customer Due Diligence for new customers, and also where the Regulated Entity otherwise feels necessary,for existing customers

i. Risk Based Approach (RBA) shall be followed for mitigation and management of the identified risk. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc.

ii. Enhanced client due diligence process shall be adopted for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. 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.

iii. KYC policies and procedures cover management oversight, systems and controls, segregation of duties, training and other related matters. For ensuring effective implementation of the KYC policies and procedures, the Regulated Entity shall prepare risk profiles of all their existing and new customers and apply Anti Money Laundering measures keeping in view the risks involved in a transaction, account or broking/business relationship.

iv. Risk Assessment: Risk Assessment shall be done 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.

v. Such Risk Assessment shall cover all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. Further, country specific information circularized by Govt of India and IFSC 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 shall be taken into account while doing risk assessment.

Enhanced Due Diligence

Where the risks of ML/TF are high, a Regulated Entity shall conduct enhanced CDD measures, consistent
with the risks identified. The enhanced CDD measures are as follows: -
(i) Obtaining additional information on the customer (e.g., occupation, volume of assets, information
available through public databases, internet, etc.), and updating more regularly the identification data of
customer and beneficial owner.
(ii) Obtaining information and taking additional steps to examine the ownership and financial position, including source of wealth and source of funds of the customer or, if applicable, of the Beneficial Owner.
(iii) Obtaining information and taking additional steps to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
(iv) Obtaining the approval of Senior Management to commence or continue the business relationship.
(v) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and,
(vi) Requiring the first payment to be carried out through an account in the customer's name with a bank
subject to similar CDD standards.

The Enhanced CDD measures will apply depending upon the risk profile of the customer and the extent of
its applicability to a customer shall be decided on case-to-case basis.
(Circumstances where a customer presents or may present a high probability of ML/TF risk may include,
but are not limited to the following:
(i) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in
relation to which the FATF has called for countermeasures; and
(ii) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the Regulated Entity for itself or notified to Regulated Entity generally by the Authority or other relevant domestic authorities in India or other foreign regulatory authorities.
(3) For establishing an account-based relationship with high-risk customers, the approval may be given by Senior Management or committee of senior managers or an individual member who has been authorized by the Senior Management in this behalf.
(4) In cases where a customer uses complex legal structures and/or trusts, private investment vehicle, the
Regulated Entity shall satisfy itself that it is used for a legitimate and genuine purpose.

(5) The Regulated Entity shall take reasonable measures to examine the source of wealth and source of funds.
That is, where the funds for a particular service or transaction will come from (e.g., a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.
(6) Source of funds refers to the origin of the particular funds or other assets which are the subject of the
establishment of business relations. In order to ensure that the funds are not proceeds of crime, the Regulated Entity should not limit its source of funds inquiry to identifying the other financial institution from which the funds have been transferred, but more importantly, the activity that generated the funds.The information obtained should be substantive and facilitate the establishment of the provenance of the
funds or reason for the funds having been acquired.
(7) Examples of appropriate and reasonable means of establishing source of funds are such as proof of dividend payments connected to a shareholding, bank statements, salary payments or bonus certificates, sale proceeds, loan documentation and proof of a transaction which gave rise to the payment into the account.
(8) A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

Simplified Customer Due Diligence

(a) Where the risks of ML/TF are low, a Regulated Entity may conduct simplified CDD measures, which should
be commensurate with the low risk factors. Examples of possible measures are:

(i) Verifying the identity of the customer and the beneficial owner after the establishment of the business
relationship .

(ii) Reducing the frequency of customer identification updates

(iii) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

(iv) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

(b) Simplified CDD (SCDD) measures shall not be conducted where there is a suspicion of ML/TF

2.5 MONITORING OF TRANSACTIONS

i. Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account. Regulated Entity shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible

lawful purpose. Transactions that involve large amount of trading activity inconsistent with the size of the balance maintained may indicate that the funds are being 'washed' through the account. High risk accounts shall be subjected to intensive monitoring. The extent of monitoring shall be aligned with the risk category of the client

ii. No Cash Transaction should be allowed. Demand Draft shall be accepted only in exceptional cases and a declaration regarding legitimate income source shall be taken from the client giving payment through Demand Draft.

iii. A register detailing date of DD, Client Code, Name, PAN, DD amount and reason for giving DD shall be maintained and reviewed to prevent frequent DD transaction from the particular client. Further, If prefunded instruments amount is more than or equal to 50,000 (or its equivalent in foreign currency) per day per client, proofs as required by IFSC are to be taken on record before acceptance of instrument.

iv. The Regulated Entity shall continue to follow strictly the instructions regarding suspicious transactions issued threshold limit of Rs.10 lakh (or its equivalent in foreign currency) and required to maintain proper record of the same.

v. A threshold limits for particular group of accounts shall be prescribed and staff shall pay particular attention to the transactions which exceed these limits. The threshold limits shall be reviewed annually and changes, if any, conveyed to Staff for monitoring.

2.6 ALERT GENERATION

i. Alert generation is a process by which the preliminary details of suspicious/unusual transactions are generated to enable the Principal Officer (PO) to analyse and review the details and arrive at a conclusion as to whether a transaction is suspicious.

ii. An alert is the first step in identification of a suspicious transaction and is a red flag which is generated arising out of a transaction. Once the alert is generated, it has to be analysed to confirm whether the transaction is ultimately suspicious or not based on the definition.

iii. Source of Alert shall be System Dependent viz placing a system to generate alerts based on certain thresholds on the transactions of the client to identify suspicious transaction and System Independent viz having a mechanism of raising alerts/triggers from employees, media reports, law enforcement agency queries etc.

iv. Efforts should be made to create awareness on reporting of unusual transactions

2.7 SUSPICIOUS TRANSACTION

i. Suspicious Transaction means a transaction whether or not made in cash which, to a person acting in good faith. 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:

- Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime
- Appears to be made in circumstances of unusual or unjustified complexity
- Appears to have no economic rationale or bona-fide purpose
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism
- Identity verification or address details seems difficult or found to be forged / false or clients that appear not to cooperate,
- Asset management services where the source of the funds is not clear or not in keeping with apparent standing /business activity
- Clients based in high risk jurisdictions;
- Substantial increases in business without apparent cause
- Unusual & Unexplained large value of transaction
- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
- Unusual & Unexplained activity in dormant accounts
- Attempted transfer of investment proceeds to apparently unrelated third parties;
- Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services

Designated/Principal Officer within the intermediary. 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.

iii. 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. The Designated/ Principal Officer and other appropriate compliance, risk management and related staff Regulated Entitys shall have timely access to client identification data and CDD information, transaction records and other relevant information.

iv. 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. All such attempted

transactions shall be reported in STRs, even if not completed by clients, irrespective of the amount of the transaction.

v. 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, shall be classified as 'CSC'. Registered intermediaries are directed that such clients shall also be subject to appropriate countermeasures. These measures may include

a. a further enhanced scrutiny of transactions,
b. enhanced relevant reporting mechanisms or
c. systematic reporting of financial transactions, and
d. Applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

3 Record Keeping

A. A Regulated Entity shall maintain the following records:
(a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
(b) reco.rds of customer business relationships (both original and certified copies), which include: -

(i) correspondence of business and other information relating to a customer's account;
(ii) adequate records of transactions to enable standalone transactions to be reconstructed; and
(iii) internal findings and analysis relating to a business transaction or other transactions, where the transaction or business may be unusual or suspicious, whether or not it results in a Suspicious Transactions Report;

(c) Suspicious Transactions Reports and any relevant supporting documents and information, including internal findings and analysis;
(d) any relevant communications, if made with the FIU;
(e) any other matter that the Regulated Entity may be expressly required to record and maintain, under these Guidelines.

B. (i) The Regulated Entity shall preserve all necessary records, for at least Eight years or for such period as prescribed under the applicable laws, from the date on which business relationship has ended ortransaction is completed.

(ii) The Regulated Entity shall provide to the Authority or any law enforcement agency immediately onrequest, a copy of a records maintained by it under these Guidelines.

(iii) Risk Assessment Documents

A Regulated Entity shall keep and maintain all risk assessment documents and provide to the Authority immediately on request, all relevant documents and information for **Appointment of Principal Officer & Designated Director**

In order to discharge legal obligation to report suspicious transaction, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Hence, Principal Officer shall be appointed and its details shall be intimated to Financial Intelligence Unit-India on an immediate basis.

The Principal Officer shall have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Principal Officer shall also have access to and be able to report to senior management above his next reporting level or the board of directors.

In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also require to designate a person as a 'Designated Director'. In terms of Section 13 (2) of the PML Act (as amended by the Prevention of Money-laundering (Amendment) Act, 2012), the Director, FIU- IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

5 Employee Hiring & Training

i. Hiring of Employees:

To ensure high standards while hiring employees, it is required that adequate screening procedures be put in place. The identification of key positions within organizational structures, considering the risk of money laundering and terrorist financing as well as the size of their business, shall be done. Moreover, the suitability and competency of employees who take up such key positions should be ensured.

Procedure that may be adopted shall include following;

All the proposed application for employment shall be taken only from the person who have valid reference of our existing staff and /or have relations with the present staff and directors.

It is prudent to also verify education and employment information which uniquely qualifies candidates for the position. In addition, it is strongly recommended that reference checks be completed prior to making the hiring decision. Further, if employee is for the post of dealer, NISM certification shall also be verified as a condition of employment.

It is strongly recommended that employment verification be completed within one week of making an offer of employment to any individual. It is strongly recommended that educational and NISM Certificate verifications be completed within one week of making an offer of employment to any individual.

After completing all the above procedures and formalities of employee screening, the company shall appoint the employee with the negotiated terms and conditions.

ii. Training of Employees

Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the Stock Broker, Commodity Broker and DP's policies and procedures to combat money laundering shall be provided to all the staff Regulated Entitys periodically in phases.

Ongoing training shall be provided to staff so that they are adequately trained in AML and CFT procedures. The KYC Department shall ensure adherence to the KYC policies and procedures. The focus of training shall be different for front office staff, back office staff, compliance staff, senior level staff and staff dealing with new customers. 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.

Further, Employees are trained with regard to compliance & Operational requirement of broking & DP entities. Also regulatory knowledge w.r.t Depositories, Stock & Commodity Exchanges, Money Laundering, etc are also imparted so that compliance & Business risk of Broker & DP are minimized.

The Regulated entity's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the policies and procedures. The compliance function shall provide an independent evaluation of the Regulated 's own policies and procedures, including legal and regulatory requirements. Concurrent/Internal Auditors shall specifically check and verify the application of AML procedures at the Regulated Entity's end and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the board on half yearly intervals.

6 Tipping off

No restriction is made on operations in the accounts where an STR has been made. Company and Our Directors, Officers and Employees are 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.

7 Customer Education

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

8 Combating Financing of Terrorism (CFT)

The Ministry of Home Affairs, in pursuance of Section 35(1) of Unlawful Activities (Prevention) Act (UAPA) 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'.

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed in the United Nations website at https://press.un.org/en/content/press-release

i. The “ISIL (Da’esh) &Al-Qaida Sanctions List”, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al- Qaida Sanctions List is available at: https://www.un.org/securitycouncil/sanctions/1267/press-releases.

ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

KYC & Surveillance department shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities. Full details of accounts bearing resemblance with any of the individuals/entities in the list are required to be intimated to IFSC and FIU-IND.

The Unlawful Activities (Prevention) Act, 1967 (UAPA) was enacted for the prevention of certain unlawful activities of individuals and associations and for matters connected therewith. UAPA has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. The Government has, since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the UAPA, relating to the purpose of prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

It is directed that stock & Commodity exchanges, depositories and registered intermediaries shall ensure expeditious and effective implementation of the procedure laid down in the UAPA Order dated August 27, 2009.

Further, GOI vide Notification dated 02/02/2021 revised earlier procedure and issued revised procedure in supersession of earlier orders and guidelines.

Implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

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 list of individuals/entities ("Designated List") shall be maintained and updated, without delay.
- Verify whether the details of entities/individuals involved in financial transactions match with the Designated List.
- Do not carry out transactions in case of a match.
- Inform the Chief Nodal Officer (CNO) (The Director FIU-INDIA Tel.No.:011-23314458, 011-23314459 (FAX) Email: dir@fiuindia.gov.in) immediately with complete details of funds, financial assets, or economic resources involved in the transaction without delay.
- A check should be run, on the given parameters, when establishing a relationship with a client and periodically thereafter to verify if individuals and entities in the Designated List hold any funds, financial assets or

economic resources, or related services such as bank accounts, stocks, and insurance policies.

- If the clients' details match with the Designated List, full particulars of the funds, financial assets or economic resources, or related services held on their books in the form of bank accounts, stocks or insurance policies etc., must be promptly informed to the CNO by stock exchanges and registered intermediaries.
- A copy of the communication specified in the above paragraphs should be sent immediately to the Nodal Officer of IFSC.
- The communication must be sent to IFSC through post and email (IFSC_uapa@IFSC.gov.in) to the Nodal Officer of IFSC, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, IFSC Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051.
- If there are reasons to believe beyond doubt that funds or assets held by a client come under the purview of Section 12A(2)(a) or Section 12A(2)(b) of the WMD Act, the individual/entity should be prevented from conducting financial transactions, under intimation to the CNO, without delay.
- A Suspicious Transaction Report (STR) covering all transactions in the accounts stated in above paragraphs, should be filed with the FIU-IND for any transactions carried out or attempted
- Upon receiving the information, the CNO would conduct verification by appropriate authorities to ensure individuals/entities' identity and funds, financial assets or economic resources comply with the Designated List.
- If the verification indicates that the assets are held for the benefit of the designated individuals/entities, the CNO would issue an order to freeze these assets under section 12A and convey to the concerned reporting entity to prohibit making any funds, financial assets or economic resources or related services available for the individuals/entities' benefit.
- Reporting entities must adhere to the provisions regarding exemptions from orders of the CNO and inadvertent freezing of accounts, as applicable.

9 Policy Review

This policy must be reviewed as and when there are regulatory amendments and in absence of any amendment, on yearly basis.

The review should ensure compliance with updated AML/CFT regulations from IFSCA, FIU-IND and any other relevant authorities.

Anti Money Laundering – Procedures

10 CUSTOMER ACCEPTANCE PROCEDURES

1) Onboarding New Clients - Offline

i. Meet the Client in Person: Before accepting the KYC, each client should be met in person at the Head Office or any of the branch offices, as per mutual convenience of the client and the organization.

ii. Verify PAN Details: PAN details of the client should be verified on the Income Tax website.

iii. Verify Documentary Proofs: All documentary proofs given by the client should be verified with the original documents.

iv. Obtain Financial Status Information: Documents like latest Income Tax returns, annual accounts, etc. should be obtained to ascertain the financial status. If required, additional information/document should be obtained from the client to ascertain their background and financial status.

v. Fill Out KYC Documents: Obtain complete information about the client and ensure that the KYC documents are properly filled up, signed and dated. Scrutinize the forms received at branch office thoroughly before forwarding it to HO for account opening.

vi. Match KYC Details with Documentary Proofs: Ensure that the details mentioned in the KYC matches with the documentary proofs provided and with the general verification done by the organization.

vii. Refuse Incomplete Information: If the client does not provide the required information, the organization should not open the account of such clients.

viii. Extra Steps for Prospective Clients: As far as possible, a prospective client can be accepted only if introduced by an existing client or associates or known entity. However, in case of walk-in clients, extra steps should be taken to ascertain the financial and general background of the client through an interview and additional financial documents such as Demat Holding, Bank Statements, Networth, Balance Sheet, etc.

ix. PoA/Mandate Holder Procedures: If the account is opened by a PoA/Mandate Holder, the relationship of the PoA/Mandate Holder with the client should be clearly ascertained. KYC and KRA procedures of such PoA/Mandate Holder must be done.

x. Refuse Benami/Fictitious Names: Accounts should not be opened where the organization is unable to apply appropriate KYC procedures, such as in the case of benami/fictitious names.

2) Continuous monitoring of Existing clients

i. Obtain the latest financial documents such as Income Tax Returns, Net worth Certificates, and Annual Accounts from the client to keep their financial status updated.

ii. Update the client's contact details, including address, phone number, demat details, and bank details. If the client cannot be contacted, try to find alternative contact details through the introducer.

iii. Conduct a background check to ensure that the client is not associated with any known criminal background or is banned in any way by any regulatory agency. Refer to websites such as www.watchoutinvestors.com for scrutiny. Prosecution Database / List of Vanishing Companies available on www.IFSC.gov.in and RBI Defaulters Database available on www.cibil.com should be checked

iv. Scrutinize the records and documents of clients belonging to special categories, such as Non-resident clients, High Net worth Clients, Trusts, Charities, NGOs, Companies having close family shareholding, Politically exposed persons, persons of foreign origin, Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange offerings, etc. Also verify UN List of Individual /Entities.

v. Review the above details regularly to ensure that the transactions conducted are consistent with the client's business, risk profile, and source of funds. Consider the country of origin and the prevalence of fraud or corruption in high-risk countries such as Libya, Pakistan, Afghanistan, etc.

11 CLIENT IDENTIFICATION PROCEDURES

a) 'Know your Client' (KYC) form, which clearly spells out the client identification procedure;

b) PAN Card is made mandatory of clients and also verified online on Income Tax site.

c) The client is identified by using reliable sources including self- attested documents / information;

d) All Documents are to be verified against the Originals.

e) Failure by prospective client to provide satisfactory evidence of identity are noted and discarded.

f) Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP and Family Regulated Entitys and Close relatives of PEPs". Following measures can be taken as enhanced due diligence in case of PEP and Family Regulated Entitys and Close relatives of PEPs.

(1) Ask the client to provide information about their sources of income, such as salary, business income, investments, and other sources of revenue.
(2) Request bank statements or other financial documents to verify the client's claimed sources of income and wealth.
(3) Conduct enhanced due diligence measures, such as conducting a background check on the client's business associates and family Regulated Entitys.
(4) Verify the client's financial history, including their past and current investments and transactions.
(5) Verify the client's reputation in the business community and their connections with influential individuals.
(6) Review any public disclosures or news reports regarding the client's financial activities or transactions.
(7) Consider the client's country of origin and whether there are any known risks associated with doing business in that country.
(8) Consider the nature and complexity of the client's transactions to identify any red flags that may indicate suspicious or illegal activity.
(9) Verify the beneficial ownership of any entities associated with the client, including the names of the directors and shareholders.

g) Conduct a background check on the client, including a check on the client's criminal record, if any.

h) Keep all client information and documents confidential and secure.

i) Conduct regular reviews of client information and documents to ensure that they remain up-to-date and accurate.

12 Digital KYC Process FOR INDIAN NATIONALS

1. The customer can initiate the digital KYC process by visiting our website or mobile application.
2. On the website or mobile application, the customer will be required to fill out an application form with all necessary personal and financial information.
3. Once the application form is completed, the customer will be required to upload scanned copies of their PAN card, Aadhaar card, and a passport-sized photograph.
4. The uploaded documents will be verified against the original records in the government's databases.
5. Once the documents are successfully verified, the customer will be asked to e-sign the application form using Aadhaar-based e-signature or any other legally valid electronic signature.
6. After the e-signature is completed, the customer will be prompted to schedule a video call with our representative for face verification.
7. Our representative will conduct the face verification process by comparing the customer's live video with the photograph uploaded during the application process.
8. If the face verification is successful, the customer will be notified that the KYC process is complete.
9. If the face verification fails, the customer will be notified about the rejection and will be asked to reinitiate the KYC process.
10. In the case where the customer visits our branch office for the KYC process, our representative will collect all necessary documents and information and initiate the digital KYC process on the customer's behalf.
11. The customer will be asked to complete the e-signature and face verification process as described in steps 5-8 above.
12. Upon successful completion of the KYC process, the customer's information will be entered into our system and updated on the relevant regulatory databases.
13. The customer will be notified that the KYC process is complete, and they can begin trading with us

For above process; following important regulatory steps and compliance to be followed

1. Develop an application for digital KYC process that is accessible to customers at touchpoints for KYC purposes. The KYC process should be conducted exclusively through this authenticated application.

2. Control access to the application, ensuring that it is only used by authorized personnel. Access to the application should be through a login-id and password or live OTP or time OTP controlled mechanism provided by the entity.

3. Customers must visit the location of authorized personnel for the purpose of KYC, and should bring their original officially valid document (OVD) with them.

4. Capture a live photograph of the customer using the application, which should be embedded in the Customer Application Form (CAF). The application must also put a watermark on the captured live photograph of the customer, which includes the CAF number, GPS coordinates, authorized official's name, unique employee code assigned by the entity, and the date and time of the photograph.

5. Ensure that only a live photograph of the customer is captured, and not a printed or video-graphed photograph. The background behind the customer should be white, and no other person should be present in the frame.

6. Capture a live photograph of the original officially valid document or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), and watermark it as mentioned above. The mobile device should not be skewed or tilted while capturing the live photograph of the original document.

7. The live photograph of the customer and their original documents must be captured in proper light so that they are clearly readable and identifiable.

8. Fill all entries in the CAF as per the documents and information furnished by the customer. In cases where Quick Response (QR) code is available in the documents, scan the QR code to auto-populate the details.

9. Send a One Time Password (OTP) message to the customer's mobile number, containing the text 'Please verify the details filled in form before sharing OTP'. The OTP will serve as the client's signature on the CAF. If the customer does not have a mobile number, a family Regulated Entity or relative's mobile number may be used, but this must be clearly mentioned in the CAF. The mobile number of the authorized officer registered with the entity must not be used for client signature.

10. The authorized officer must provide a declaration about capturing the live photograph of the customer and the original document. Verify the authorized

officer with an OTP sent to their registered mobile number, and capture their live photograph as well. The OTP will serve as the authorized officer's signature on the declaration.

11. Upon completion of the process, the application should provide information about the submission of the activation request to the activation officer of the entity, and generate a transaction- id/reference-id number for the process. The authorized officer should communicate this number to the customer for future reference.

12. The authorized officer should verify that the information available in the picture of the document matches the information entered in the CAF, the live photograph of the customer matches the photo in the document, and all mandatory fields are filled properly in the CAF.

13. If the verification is successful, the CAF should be digitally signed by an authorized representative of the entity. The authorized representative should take a print of the CAF, obtain the customer's signatures/thumb impression in the appropriate place, scan and upload the CAF in the system, and return the original hard copy to the customer.

13 Risk Categorization /PROFILING

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF INDIVIDUALS

Type	Recommended Risk Categorization	Risk Perception
Salaried	Low risk	Source on income is fixed and pattern of entries in the account can be correlated with known sources of income/ expenditure. This means that their financial transactions are more transparent and less likely to be associated with money laundering or other illicit activities. As a result, financial institutions can conduct simplified due diligence and monitoring procedures for these accounts compared to accounts of higher-risk clients.
Senior citizens	Medium / High Risk	Source of income for trading related purposes may not be clear, and the account may be operated by third parties. Additionally, if the individual is involved in trading in the F&O segment, it will be considered a high-risk account. However, if the individual is dealing only in the CM segment for IPOs, then the risk categorization can be lowered to low risk. The risk perception is higher for senior citizens as they may not have a regular source of income and may be more vulnerable to financial frauds and scams.
House-wife	Medium / High Risk	Source of income for trading related purposes not known clearly. May be operated by third parties. Will be considered high risk in case operating in F&O. If dealing only in CM Segment for IPOs then Low Risk.

Self Employed-Professionals/ Businessmen	Low risk (except professionals associated with the film industry who will be categorized as "Medium" risk).	Accounts maintained by Chartered Accountants, Architects, Doctors, Lawyers, Sports men, etc. However, professionals associated with the film industry may be categorized as "Medium" risk due to the nature of their work and the potential for high- value transactions. The film industry is known for its cash-based transactions, and the source of income for professionals in this industry may not always be clear or easy to trace, making them more susceptible to potential risks.

Non Resident Individuals	Low / Medium risk	Transactions are regulated through AD and the accounts are opened only after IPV. In case an IPV is not performed and we have relied on documentation submitted by the client, the account would be categorized as medium risk.
Politically Exposed Persons resident outside India	High Risk	Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Front end staff should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Such accounts should be subjected to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family Regulated Entitys and close relatives of PEPs. Further company may maintain a list of additional accounts as "Designated PEP" The accounts of Politically Exposed Persons resident outside India shall be opened only after obtaining the approval of Business Head. Further, in the event of an existing customer or the beneficial owner of an account subsequently becoming PEP, Business head approval would be required to continue the business relationship and such accounts would be subjected to Customer Due Diligence measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. In such events Company shall be guided by the information provided by the clients or front end teams.

NOTE: If any of the above accounts are operated by Power of Attorney (POA) holder/mandate holder, then the account will be categorized as "High Risk". Further, Compliance Officer after consultation with Director has right to lowering of Risk categorization , however such lower classification shall be reviewed after 3 months from the date of account opening or date of first trade.

RISK CATEGORISATION FOR ACCOUNTS IN THE NAME OF NON- INDIVIDUALS

Risk categorization of Non Individual customers can be done basis:

A. Type of Entity

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

Trusts – Private Trust	High Risk	These may be unregistered trusts and the pattern of entries in the account may not be correlated with known sources of income/ expenditure.
Co-operative Banks	High Risk	These are not highly regulated entities.

B. Basis Industry

Categorization	Nature of Industry
High	The Risk categorization is dependent on industries which are inherently High Risk or may exhibit high cash intensity, as below: Arms Dealer Money Changer Exchange Houses Gems / Jewellery / Precious metals / Bullion dealers (including sub- dealers) Real Estate Agents Construction Offshore Corporation Art/antique dealers Restaurant/Bar/casino/night club Import/Export agents (traders; goods not used for own manufacturing/retailing) Share & Stock broker Finance Companies (NBFC) Transport Operators Auto dealers (used/ reconditioned vehicles/motorcycles) Scrap metal dealers Liquor distributorship Commodities middlemen Co-operative Banks Car/Boat/Plane dealerships/brokers Multi-Level Marketing (MLM) Firms
Medium	None
Low	All other industries

Notes:

1 Higher Risk Categorization derived from either A or B or C shall be the applicable risk categorization for the account.

2 Lowering of risk classification shall be carried out by the Compliance officer in consultation with the either Principal Officer or Designated Director as reported to FIU.

3 Based on the above categorization the transaction review process will take place.

4 Additionally, in case an account is opened wherein a POA to operate the account is provided to another person who is not family Regulated Entity. Such accounts shall be placed under the High Risk category.

13.1 OPENING OF IBT/WT TRADING ACCOUNTS

After proper customer acceptance & identification procedures for opening of trading account, if client requires IBT/Wireless facility, a written request shall be taken if he has not opted for said facility through KYC.

We make sure that such clients are literate and have understood the rights and obligation with regard to Internet/wireless Trading.

14 AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES

(a) Detect Suspicious indicators

The first step in identifying a suspicious transaction is to detect indicators that a transaction(s) may involve funds that are derived from an illegal activity or that the transaction(s) is an attempt to disguise funds derived from illegal activity or lacks a business or apparent lawful purpose.

1) The suspicious indicators act as "red flags" and alerts for the Regulated Entity to pay more attention to a particular customer or transaction(s). These indicators include:

(a) complex, unusual or large transactions that have no apparent economic or lawful purpose;

(b) unusual pattern of transactions that have no apparent economic or lawful purpose;

(c) the transaction (or attempted transaction) does not match the known background, nature and

(d) unusual customer behaviour;

(e) Customers whose identity verification seems difficult or clients that appear non-cooperative;

(f) Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;

(g) Customers based in high-risk jurisdictions;

(h) Substantial increases in business without apparent cause; or

(i) Attempted transfer of investment proceeds to apparently unrelated third parties.

2) The presence of suspicious indicators does not immediately equate to criminality or suspicion. Rather, the detection of an indicator, especially a combination of indicators, should prompt the Regulated Entity to increase monitoring and to take further actions to assess whether the transaction(s) should be reported to the FIU-IND as suspicious.

Ask Customer Questions

(i) If one or more suspicious indicators are detected, the Regulated Entity and its employees may ask the customer relevant and appropriate questions to determine whether there is a reasonable explanation for that observed indicator.

(ii) The Regulated Entity shall ensure that when asking such questions, they do not "tip-off" the customer.Instead, questions could be asked using a service approach.

Review Customer's Records

The next step is to determine whether the suspicious indicators identified earlier is justifiable given what is known about the customer. To achieve this, a Regulated Entity shall review its customer's records and consider all information that is already known to it about the customer. This may include:

(i) the customer's usual occupation, business or principal activity;

(ii) the customer's transaction history;
(iii) the customer's risk profile;
(iv) the customer's income level;
(v) the customers source of income as stated during account opening or initial engagement;
(vi) reasons for the transactions as provided by the customer;
(vii) the "relationship" of the customer with the sender or beneficiary of funds;
(viii) the frequency of transactions;
(ix) the size and complexity of the transaction;
(x) the identity or location of any other person(s) involved in the transaction;
(xi) the usual or typical financial, business or operational practices or behavior of customers in the similar occupation or business category; and
(xii) the availability of identification documents and other documentation. After reviewing as aforesaid if the Regulated Entity finds that the customer's profile has changed, it shall update the customer's profile.

(d)Evaluate Information Collected.

A Regulated Entity shall evaluate the:
((a)(i) suspicious indicators,
(ii) information solicited from the customer through questions asked, and
(iii) known information about the customer to determine if there are reasonable grounds to suspect thatthe transaction(s) is related to the commission of a ML/ TF or any other serious offence.
(b) If the Regulated Entity concludes that there are reasonable grounds to suspect that the transaction(s)or attempted transaction(s) is linked to a ML/ TF or any other serious offence, it should report this suspicion to the FIU-IND by completing and submitting a STR.

3 Quarterly MIS of the number of alerts received, reviewed, pending and escalated would be reported to the Board in the Board Meeting. Reason for pendency beyond the closure date would be explained.

4 Compliance department would be responsible for independent oversight of the compliance with these requirements.

16 COMPLIANCE OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS AND DOMESTIC LAWS

11.1. Requirements/obligations under International Agreements Communications from International Agencies –
(a) The Regulated Entities shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have

any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

(i) The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

(ii) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at: https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/ resources/xsl/en/taliban-r.xsl

(b) Details of accounts resembling any of the individuals/entities mentioned in the above lists, shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021, issued by the CTCR Division of the Ministry of Home Affairs, Government of India, which is available at https://www.mha.gov.in/sites/default/files/ProcedureImplementationSection51A_30032021.pdf

(c) In addition to the above, other UNSC Resolutions circulated by the IFSCA in respect of any other jurisdictions/ entities from time to time, shall also be taken note of for necessary compliances.

17 Freezing of financial assets:

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order bearing file no.14014/01/2019/CFT dated February 2, 2021,
issued by the CTCR Division of the Ministry of Home Affairs, Government of India, shall be strictly
followed and compliance with the Order shall be ensured. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs18 Procedure for unfreezing

- 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 regulated entities shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing that the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Central [designated) Nodal Officer for UAPA within two working days.
- The Central [designated) Nodal Officer for UAPA, 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, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned regulated entities and registered intermediaries. However, if it is not possible for any reason to pass an order unfreezing the assets within five working days, Central [designated) Nodal Officer for UAPA shall inform the applicant.

19 FATF Recommendations

- The Financial Action Task Force (FATF) is an intergovernmental organization established to combat money laundering, terrorist financing, and other threats to the integrity of the international financial system. The FATF sets international standards and recommendations for anti-money laundering and countering the financing of terrorism (AML/CFT).
- The FATF Recommendations are a comprehensive set of measures designed to provide a framework for countries to implement effective AML/CFT policies and procedures. The Recommendations cover a wide range of issues, including customer due diligence, record-keeping, reporting of suspicious transactions, and international cooperation.
- The FATF Recommendations are widely recognized as the global standard for AML/CFT and are implemented by over 200 countries and jurisdictions worldwide. The FATF regularly reviews and updates its Recommendations to address emerging threats and ensure that they remain relevant and effective in combating money laundering and terrorist financing.
- The Financial Action Task Force (FATF) Secretariat issues public statements after each plenary to address strategic deficiencies in countries' regimes for countering money laundering, terrorist financing, and proliferation financing risks. The Securities and Exchange Board of India (IFSC) will circulate the FATF statements, and registered intermediaries must consider publicly available information to identify countries that inadequately apply the FATF Recommendations.
- Registered intermediaries must take into account the risks that arise from deficiencies in the anti-money laundering/combating the financing of terrorism (AML/CFT) regimes of countries mentioned in FATF statements. However, it is important to note that regulated entities may still engage in legitimate trade and business transactions with these countries and jurisdictions.

20 REPORTING

In terms of the PML Rules, intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India(FIU-IND) at the following address:

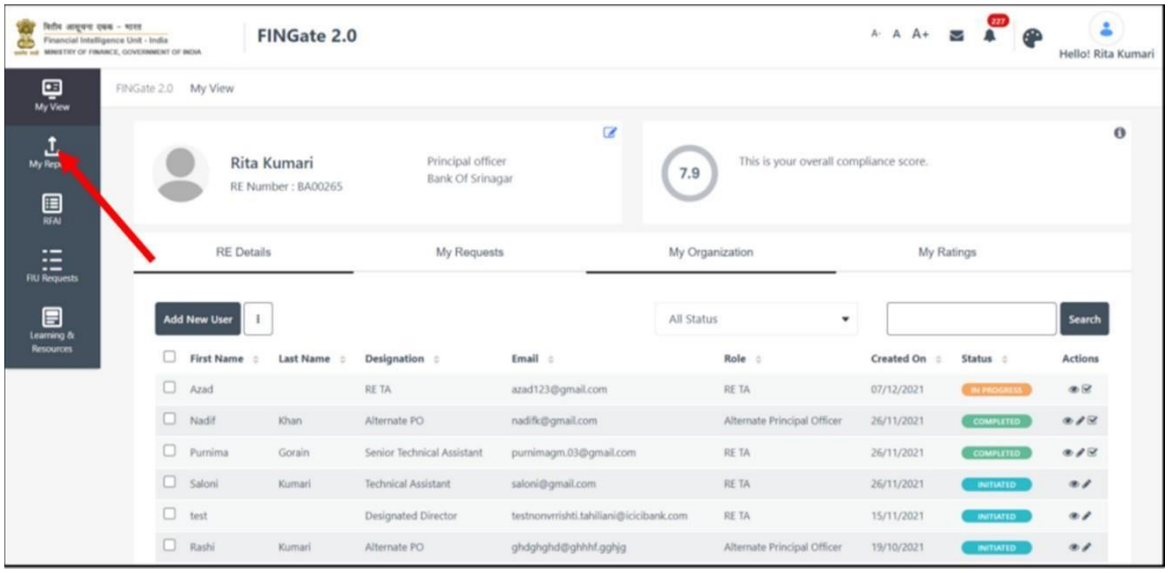
Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

Reporting and Reports are to be done to FIU as per Procedures laid down in FINnet 2.0 is implemented as a set of three (3) systems to ensure that the data ingested and processed by the three is isolated and immune to security threats as much as possible and all data is secure.

The systems are listed below –

1. FINGate – Collection and preprocessing system
2. FINCore – Processing and analysis system
3. FINex – Dissemination system

The FINGate system consists of multiple reporting mechanisms to ensure compliance and facilitate quick and easy reporting.



Overview of 'Report dashboard navigation and action

For detailed User Manual of Fin NET Portal is as per link

https://fiuindia.gov.in/files/misc/finnet2.html

Disclaimer & Review

This policy & Procedure must be reviewed as and when there are regulatory amendments and in absence of any amendment, on yearly basis. The information contained in this material is intended only for the use of the entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally privileged information. The addressee is hereby notified that any disclosure, copy, or distribution of this material or the contents thereof may be unlawful and is strictly prohibited.