ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER POLICY

applicable to

T-CAP FINANCIAL SERVICES IFSC PRIVATE LIMITED
("**T-CAP**")

Document Change Control

Version	Policy	Reviewed Date	Department	Approved by
V1	Anti-Money Laundering and Know Your Customer Policy	First Policy	Compliance	Pranav Inamdar (Director of the Company

I N D E X

Sr. No.	Particulars	Page No.
1.	Introduction	4
2.	Objective	5
3.	Scope	5
4.	What is Money Laundering?	5
5.	Definitions	6
6.	Salient Provisions of the Prevention of Money Laundering Act, 2002	11
7.	Policy and procedures to Combat Money Laundering and Terrorist Financing of T-Cap.	11
8.	Policies and procedures to combat ML and TF covers	13
9.	Written Anti Money Laundering Procedures	13
10.	Implementation of this Policy	13
11.	Scope of the Guidelines	14
12.	Steps for Implementing the Policy	14
	I. Risk Based Approach	14
	II. Business Risk Assessment	15
	III. Customer Risk Assessment	16
	IV. Client Due Diligence	18
	V. Client Identification Procedure	20
	VI. Reliance on Third Party for carrying out Client Due Diligence (CDD)	25
	VII. Use of Business Facilitator	26
	VIII. Monitoring of Transactions	27
	IX. Suspicious Transaction Monitoring and Reporting	28
	X. Reporting to Financial Intelligence Unit-India	29
	XI. Record Management	30
	XII. Retention of records	32
13.	Policy Review	37
14.	Deviation to Framework	37
15.	Power to Remove Difficulties	37
16.	Effective Date	37
17.	Annexure 1	38
18.	Annexure 2	41
19.	Annexure 3	47
20.	Annexure 4	50
21.	Annexure 5	54

ANTI-MONEY LAUNDERING POLICY

1. **Introduction**

T-Cap Financial Services IFSC Private Limited (CIN:U65990GJ2018PTC104040) ("**T-Cap**") is a private company incorporated under the provisions of the Companies Act, 2013 having its registered office at Unit 618, Signature Building, 6th Floor, Block- 13B, Zone -1, Gift City Gandhinagar, Gujarat – 382355 and is engaged in the business of fund management activities (Non-retail).

The Prevention of Money Laundering Act, 2002 ("**PMLA**") was brought into force with effect from July 01, 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on July 01, 2005.

Subsequently, International Financial Services Centres Authority (IFSCA) issued International Financial Services Centres Authority (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 ("**IFSCA Guidelines**") vide Notification no. IFSCA/2022-23/GN/GL001.— dated 28th October, 2022, (Updated as on February 26, 2026)

The provisions of these Guidelines shall apply to every Regulated Entity which is licensed, recognised or registered by IFSCA and also to the Regulated Entities authorised by it, to the extent specified.

The provisions of these Guidelines shall also apply to a Financial Group of the Regulated Entity, to such extent as specified in Chapter-XII of the Guidelines.

Duties of a Regulated Entity

(a) Every Regulated Entity shall formulate an AML-CFT policy, which shall be duly approved by the Governing Body or by a committee to whom such power has been delegated by the Governing Body. While formulating the AML-CFT policy, every Regulated Entity shall incorporate the key principles or elements of these Guidelines.

(b) Additionally, every Regulated Entity shall develop a KYC Policy which shall be the part of its AML-CFT policy.

(c) Every member of Regulated Entity's Senior Management shall be responsible for the Regulated Entity's compliance under these Guidelines. While carrying out their responsibilities under these Guidelines every member of a Regulated Entity's Senior Management shall exercise due skill, care, and diligence.

Accordingly, T-Cap, being the entity registered in IFSC, has prepared its own Anti Money Laundering Policy as per IFSCA Guidelines on Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer under the Prevention of Money Laundering Act, 2002 and Rules Framed thereunder and amendments thereto which has been duly approved by the Directors of the T-Cap.

Further, the T-Cap will also undertake the implementation of the IFSCA Guidelines for its fund in IFSC through this policy.

Geninnov Trust Global Innovation Fund ('**Fund**'), having its registered office at Unit No. 618, Signature Building, 6th Floor, Block 13B, Zone – I, GIFT SEZ, GIFT – City, Gandhinagar, 382355, has been launched as a Restricted Scheme (Non-retail) i.e. Category III Alternative Investment Fund ('**AIF**') in accordance with IFSCA (Fund Management) Regulations, 2022 in IFSC at GIFT City. The Fund has been launched by T-Cap Financial Services IFSC Private Limited which is registered as a Fund Management Entity ('**FME**').

T-Cap Financial Services IFSC Private Limited has also obtained registration as a Investment Banker ('**IB**') with the Securities and Exchange Board of India ('**SEBI**') in accordance with SEBI (FPI) Regulations, 2019.

2. Objective

The objective of this policy framework is to:

i. Create awareness and provide clarity on KYC standards and AML measures.
ii. Outline the obligations under PMLA.
iii. Provide a framework for systems and procedures.
iv. To prevent criminal elements from using our business for money laundering activities
v. To understand the customers and their financial dealings better, which in turn would help the company to manage the risk prudently.
vi. To put in place appropriate controls for detection and reporting suspicious transactions in accordance with applicable laws/ laid down procedures.
vii. To adopt Risk Based Approach (RBA) to identify and assess the Money Laundering (ML) and Terrorist Financing (TF) risk to which T-Cap and its customers are exposed depending upon the nature and size of its investment activities; and
viii. undertake business risk assessment and customer risk assessment based on Risk Based Approach.

3. Scope

These policies and procedures apply to all employees and Directors of T-Cap and are to be read in conjunction with the existing guidelines. The procedures prescribed hereunder have been established to ensure that all employees and Directors know the identity of their customers and take appropriate steps to combat money laundering.

This document containing policy and procedures on Anti-Money-Laundering has been drafted as a compendium of all the circulars and guidelines which were circulated previously. This has been prepared for ease of reference and proper dissemination across T-Cap for implementation of the Guidelines.

As provided in the Guidelines/ Rules, the Policy identifies the major areas of activity related to dealing with clients such as customer identification and acceptance, reporting of suspicious transactions and maintenance of records for implementation by T-Cap.

The Policy mainly focuses on:

i. Risk Based Approach
ii. Business Risk Assessment
iii. Customer Risk Assessment
iv. Client Due Diligence
v. Client Identification Procedure

vi. Reliance on Third Party for carrying out Client Due Diligence (CDD)
vii. Use of Business Facilitator
viii. Monitoring of Transactions
ix. Suspicious Transaction Monitoring and Reporting
x. Reporting to Financial Intelligence Unit-India
xi. Record Management
xii. Retention of records
xiii. List of Designated Individuals/ Entities
xiv. Procedure for freezing of funds, financial assets or economic resources or related services
xv. Jurisdictions that do not or insufficiently apply the FATF Recommendations
xvi. Designation of officers for ensuring compliance with provisions of PMLA
xvii. Hiring and Training of Employees, Investor Education and Audit function
xviii. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR)

The above-mentioned functions shall be suitably assigned to the departments which handle the respective activities.

4. **What is Money Laundering?**

Money Laundering may be defined as cleansing of dirty money obtained from legitimate or illegitimate activities including drug trafficking, terrorism, organized crime, fraud and many other crimes with the objective of hiding its source and rendering it in legally usable form. It is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. The process of money laundering involves creating a web of financial transactions so as to hide the origin of and true nature of these funds.

This is done in below three phases:

A. Placement Phase – The first stage in the process is placement. The placement stage involves the physical movement of currency or other funds derived from illegal activities to a place or into a form that is less suspicious to law enforcement authorities and more convenient to the criminal. The proceeds are introduced into traditional or non-traditional financial institutions or into the retail economy.

B. Layering Phase – The second stage is layering. The layering stage involves the separation of proceeds from their illegal source by using multiple complex financial transactions (e.g., wire transfers, monetary instruments) to obscure the audit trail and hide the proceeds.

C. Integration Phase – The third stage in the money laundering process is integration. During the integration stage, illegal proceeds are converted into apparently legitimate business earnings through normal financial or commercial operations. Having identified these stages money laundering process, financial institutions are required to adopt procedures to guard against and report suspicious transactions that occur in any stage.

Section 3 of the PMLA defines money laundering in following words:

“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.”

Financial Intelligence Unit (FIU) – INDIA

The Government of India had set up Financial Intelligence Unit (FIU-IND) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND 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.

5. **Definitions:**

A. "Act" and "Rules" means the Prevention of Money-laundering Act, 2002 and the Prevention of Money- laundering (Maintenance of Records) Rules, 2005, respectively

B. "Authority" or "IFSCA" means the International Financial Services Centres Authority established under sub-section (1) of section 4 of International Financial Services Centres Authority Act, 2019 (50 of 2019).

C. Beneficial Owner means-

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has a controlling ownership interest or who exercises control through other means.

i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent. of the shares or capital or profits of the company
ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements

b. Where the customer 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/have ownership of/entitlement to more than ten per cent. of capital or profits of the partnership

c. Where the customer 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/have ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals;
Explanation: The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent. 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.

D. "Business Facilitator" means a person authorised by the Regulated Entity, to verify the information/officially valid documents provided by the customer for opening account with it

E. "Central KYC Records Registry" means an entity defined under rule 2 (1) (ac) of the Rules, which is authorised to receive, store, safeguard and retrieve the KYC records of a customer in digital form.

F. "Certified Copy" means comparing the original officially valid document provided by the customer with the copy thereof and recording the same as 'true copy' by the authorised officer of the Regulated Entity.

Provided that in case of non-resident individuals including Non-Resident Indians (NRIs), the certification may be carried out by:

i. Authorised official of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship;
ii. Notary Public (outside India);
iii. Court Magistrate (outside India);
iv. Judge (outside India);
v. Certified public or professional accountant (outside India);
vi. Lawyer (outside India);
vii. The Embassy/Consulate General of the country of which the non-resident individual is a citizen; or
viii. Any other authority as may be specified by the Authority.

G. "Designated Director" means a person designated by the Regulated Entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act, the Rules and these Guidelines

H. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Regulated Entity as per the provisions contained in the Act.

I. "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 customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 or its equivalent in other jurisdictions, as may be recognised by the Authority.

J. "Financial Group" means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level

K. "Financial Intelligence Unit – India" refers to a national agency, set by the Government of India, which is inter-alia responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions.

L. "Money Laundering" shall have the meaning assigned to it under section 3 of the Act and "Anti-Money Laundering" shall be construed accordingly, and shall include Counter-Terrorist Financing and other related measures.

M. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Regulated Entity or meeting the authorised officials/persons of the Regulated Entity.

N. "Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)

O. "Non- Resident Indian" shall have the meaning as defined in Foreign Exchange Management (Deposit) Regulations, 2016.

P. "Officially Valid Document" means the passport, the driving license, proof of possession of Aadhar number, the Voter's Identity Card issued by the Election Commission of India or 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;

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

Provided further that, where simplified measures are applied for verifying the identity of the customers, the following documents shall also be deemed to be 'officially valid document': -

(a) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
(b) letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided also that where the simplified measures are applied for verifying the limited purpose of proof of address of the customer, where a prospective customer is unable to produce any proof of address, the following document shall also be deemed to be Officially Valid Document:

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property, Municipal tax receipt, city council tax receipt, or such other equivalent document;
iii. Post Office savings bank account statement or statement of a bank account including of a foreign bank;
iv. pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
v. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector

undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation; and

Provided also that in case the Officially Valid Document presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address;

Provided also that where the client submits his proof of possession of Aadhaar number as an Officially Valid Document, he may submit it in such form as are issued by the Unique Identification Authority of India.

Q. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the Customer Due Diligence process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity specified by the Authority

R. "Principal Officer" means an officer designated by the Regulated Entity as such, who shall be responsible for furnishing information as required under rule 8 of the Rules.

S. "Politically Exposed Person" means the individuals who are or have been entrusted with prominent public functions by any country, which shall include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials or International Organisation Politically Exposed Person.

Explanation: The definition of Politically Exposed Person is not intended to cover middle ranking or more junior individuals in the definition

T. "Regulated Entity" means a unit/entity which has been granted license, recognition, registration or authorisation by the Authority.

U. Senior Management" means

a. In relation to a Regulated Entity,
   (i) for an incorporated entity in International Financial Services Centre in India, every member of the Regulated Entity's Governing Body;
   (ii) for a branch, the person or persons who control the day-to-day operations of the Regulated Entity in an IFSC and may include such other persons as may be designated by the Regulated Entity.

b. In relation to a customer, that is a legal person, every member of its Governing Body and the person or persons who control its day-to-day operations.

V. "Suspicious Transaction" means a "Transaction" as defined in these Guidelines, including an attempted transaction, which to a person acting in good faith-

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

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

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

a. opening of an account;
b. deposits, withdrawal, exchange or transfer of funds in whatever currency, whether by payment order or other instruments or by electronic or other non-physical means;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; and
f. establishing or creating a legal person or legal arrangement.

X. "Video based Customer Identification Process" or "V-CIP" means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the Regulated Entity, by undertaking seamless, secure, live, informed &consent based audio-visual interaction with the customer to obtain identification information required for Customer Due Diligence purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

6. **Salient Provisions of the Prevention of Money Laundering Act, 2002**

Sec 3 - Offence of money-laundering:

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 proceeds or crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.

Sec 4 - Punishment for money-laundering

Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine.
Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule (Offences under The Narcotic Drugs and Psychotropic Substances Act, 1985), the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted.

7. **Policy and procedures to Combat Money Laundering and Terrorist Financing of T-Cap**

A. Essential Principles:

a) These Directives have taken into account the requirements of the PMLA as applicable to the regulated entity which has been granted license, recognition, registration or authorisation by IFSCA. The detailed Directives have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall consider carefully the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures and the requirements as laid down in the PMLA and guidelines issued by the Government of India from time to time.

b) In case there is a variance in Client Due Diligence (CDD)/Anti Money Laundering (AML) standards specified by IFSCA and the regulators of the host country, T-Cap shall require its respective entity in that jurisdiction to apply the higher of the two standards, to the extent permitted by the law of that jurisdiction.

c) If the law of host country does not permit the proper implementation of KYC/AML-CFT standard measures consistent with the home country requirements, T-Cap shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform IFSCA

d) Where the T-Cap has a branch or subsidiary in a country or jurisdiction:

(i) For which the FATF has called for countermeasures; or

(ii) It is known to have inadequate AML/CFT measures, as identified by the T-Cap for itself or notified by the IFSCA or other foreign regulatory authorities to the Regulated Entities;

T-Cap shall ensure that its group policy on KYC-AML-CFT standards is strictly observed by the management of that branch or subsidiary.

B. Obligation to establish policies and procedures:

a) Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that T-Cap shall ensure the fulfilment of the aforementioned obligations.

T-Cap shall be required to implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the financial group as under [“group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of rule 2 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 as amended from time to time:

i. has developed and implemented its group policies and procedures for the sharing of information between Financial Group entities, including the sharing of information related to CDD and for ML/TF risk management;

ii. has put in place adequate safeguards to protect the confidentiality and use of any information that is exchanged between Financial Group entities;

iii. remains aware of the ML/TF risks of the Financial Group as a whole, of its exposure to the Financial Group and takes active steps to mitigate such risks;

iv. contributes to a Group-wide risk assessment to identify and assess ML/TF risks for the Financial Group;

v. provides its Group-wide compliance, audit and AML/CFT functions of customer, account, and transaction information from its branches and subsidiaries, when necessary for the purposes of ML/TF risk management

b) To be in compliance with these obligations, the senior management of T-Cap shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. T-Cap shall:

i. issue a statement of policies and procedures and implement, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements

ii. ensure that the content of these Directives are understood by all staff members;

iii. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;

iv. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;

v. undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;

vi. have a system in place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and

vii. develop staff members' awareness and vigilance to guard against ML and TF

8. **Policies and procedures to combat ML and TF covers**

a) Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
b) Following a Risk Based Approach to combat ML / TF
c) Business Risk Assessment
d) Customer Risk Acceptance including Client acceptance policy and client due diligence measures, including requirements for proper identification;
e) Maintenance of records;

f) Compliance with relevant statutory and regulatory requirements;
g) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
h) Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard; and,
i) The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.
j) Compliance obligations under International Agreements and domestic laws.
k) T-Cap shall comply with obligations under UNSC resolutions, FATF recommendations, and domestic laws like UAPA, including sanctions screening and reporting of NTRs for NPOs.

9. **Written Anti Money Laundering Procedures**

T-Cap adopted written procedures to implement the anti-money laundering provisions as envisaged under the PMLA. This procedure includes, inter alia, the following four specific parameters which are related to the overall 'Client Due Diligence Process':

i. Risk Based Approach
ii. Business Risk Assessment
iii. Customer Risk Assessment and
iv. Client Acceptance Policy
v. Client Due Diligence
vi. Client Identification Procedure - procedure for identifying the clients and the ultimate beneficial owners and verifying such information;
vii. Monitoring of Transactions

T-Cap would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a framework for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to FIU as per the guidelines of PMLA Rules, 2002.

10. **Implementation of this Policy**

Designated Director and Principal Officer shall ensure compliance of the provisions of the IFSCA Guidelines along with the provisions of the Act and the Rules to the extent applicable as a central reference point and play an active role in identification & assessment of potentially suspicious transactions.

11. **Steps for implementing the policy**

A. **Risk Based Approach**

T-Cap has a Risk Based Approach ("**RBA**") for mitigation and management of the identified risk and has policies approved by their senior management, controls and procedures in this regard. T-Cap monitor the implementation of the controls and enhance them if necessary.

RBA is to be undertaken at two levels:

a) Business Risk Assessment – assessing risk on various parameters based on nature and size of its business activities to which the entity itself is exposed.
b) Customer Risk Assessment – assessing risks of each customer (new as well as existing) and assigning risk rating (high / medium / low) based on such assessment. The purpose of this risk classification is to apply adequate level of customer due diligence based on the risk category of each customer.

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. As such, T-Cap applies each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that T-Cap adopts an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that T-Cap obtains necessarily depend on the risk category of a particular client.

T-Cap does not apply low risk provisions 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.

B. **Business Risk Assessment**

Business Risk Assessment is undertaken to determine T-Cap's own susceptibility to ML/TF risks. This helps to understand its exposure to ML/TF risks and take necessary steps to mitigate them.

T-Cap carries out risk assessment 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.

T-Cap carries out risk assessment after considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment is documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

T-Cap shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. T-Cap shall ensure:

a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
b. Adoption of a risk based approach to manage and mitigate the risks

T-Cap while carrying out risk assessment takes into account any country specific information that is circulated by the Government of India and IFSCA from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

C. **Customer Risk Assessment (CRA)**

Categorization of the customers into high, medium and low risks customers decides the degree of CDD to be undertaken. Degree of CDD is divided into three categories:

(a) Simplified CDD – for low-risk customers
(b) Normal CDD – for medium risk customers
(c) Enhanced CDD – for high-risk customers

For undertaking CRA, T-Cap will:

a) identify the customer and beneficial owner;
b) take into consideration customer's country of origin, residence, nationality, place of incorporation or place of business, nature of business relationship; and
c) Obtain any other information, as may be required and deemed fit from time to time.

Below are some of the indicative factors which will be taken into consideration before assigning the risk rating (high/medium/low) to each customer:

High Risk factors:

a) Unusual or complex ownership structure / legal structure
b) Non-face-to-face business relationships or transactions, without adequate safeguards
c) Anonymous transactions in which payments are received from unknown or unassociated third parties
d) Jurisdictions which are considered as high risk under FATF recommendations
e) Any other factors as may be relevant

Low Risk Factors:

a) Government entity of a non-sanctioned jurisdiction or an associate / affiliate / related entity
b) Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership
c) Regulated Financial institutions (including subsidiaries) incorporated or established outside India subject to AML / CFT requirements set by FATF;
d) Countries or jurisdictions not identified in the above parameters for 'High risk' categorization
e) Any other factors as may be relevant

D. **Client Acceptance Policy**

T-Cap has developed client acceptance policies and procedures that aim to identify the types of clients that are likely to pose higher than average risk of ML or TF. By establishing such policies and procedures, we will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. The following safeguards are followed while accepting the clients:

a) Once the client meets the acceptance norms, a recommendation on the account opening form shall be given by the Authorised person/ branch manager/ relationship manager, to open the account.

b) No account is opened in anonymous or fictitious/ benami name(s). To prevent the opening of account in fictitious or benami name on behalf of other persons whose identity has not been disclosed or cannot be verified, following steps shall be taken:

   i. The signature of the client is verified with the signature appearing on the proof of photo identity (PAN card).
   ii. The details of PAN card are cross-verified from the Income-Tax website.
   iii. The client personally submits the relevant documents to the relationship manager/ authorised person.
   iv. The KYC and necessary agreements/undertakings are signed by the client himself. Under no circumstances, account shall be opened on the basis of the signature of Power of Attorney holder.

c) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher; Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

d) No client account is opened where it is not possible to apply appropriate client due-diligence measures/ policies e.g. ultimate beneficial owners not identifiable, suspected non genuine/incomplete information, client's non-co-operation, incomplete KYC form, non-availability of documents with the client, reluctance of client to personally meet the officials etc.

e) No client account shall be opened for shell financial institution

f) Where a client fails to provide such information, the matter shall be reported to the appropriate higher authority.

g) Reasonable enquiries are made about the client's background to ensure that the client/Beneficial owner does not have a criminal background or is not banned in any manner, whether by way of criminal or civil proceedings by any enforcement agency in India or abroad. For this purpose, the following steps shall be taken:

   i. Check the client name, PAN, address, email id, contact details etc. in the relevant database or client screening database or negative list to verify the criminal background of the client
   ii. In case of any match, account is not opened for such client unless the verification of suitability of acceptance of the client is done.

h) New account opening application will be validated with various watch lists including but not limited to the RBI watch list/other available checklists to ascertain the

creditworthiness of the Client and to check whether the name of the client appears on the UNSCR list, MHA list or FATF list or client is PEP.

i. To facilitate this, 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 United Nations' Security Council Resolutions (UNSCRs) can be accessed in the United Nations website
ii. Wherever any employee of T-Cap dealing with the Client or a prospective Client has a reason to believe that the Client should be categorized as 'high risk' client and therefore needs a higher degree of due diligence and regular update of KYC profile, he shall bring the same to the notice of the 'Principal Officer' as defined in this document.

Relationship Manager and Customer Service Manager are required to maintain continuous familiarity and follow up where any inconsistencies are noticed in the information provided with respect to any account being opened

E. **Client Due Diligence**

Keeping in view the guidelines, the following activities shall be performed by the account opening departments such as the mid-office of business team, authorized branches etc.:

a) Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

b) Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or T-Cap, T-Cap shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person. Provided that in case of a T-Cap, the T-Cap shall ensure that trustees disclose their status at the time of commencement of an account based relationship.

c) Identifying beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted.

d) Where the T-Cap has exhausted all possible means but has not been able to identify the Beneficial Owners, it shall treat the Senior Management of the said legal person or legal arrangement, as the Beneficial Owner

e) Exemption from identification of Beneficial owner: Where the client or the owner of the controlling interest is a company listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary

of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies unless the T-Cap has doubts about the veracity of client due diligence information, or suspects that customer may be connected with ML/TF.

The jurisdictions notified by Central Government are United states of America, Japan, South Korea, United Kingdom excluding British Overseas Territories, France, Germany, Canada.

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

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

h) Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the T-Cap knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.

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

j) T-Cap shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

k) T-Cap shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of six years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is late

l) Where T-Cap is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, T-Cap shall not pursue the CDD process, and shall instead file a STR with FIU-IND

m) Documentary evidence and details as per "Know Your Client" guidelines issued by IFSCA to be read in line with PMLA 2002 shall be sought from the client to establish the identity of the client.

n) Each original document shall be seen prior to acceptance of its copy by the relationship managers/branch managers/authorised persons and the same shall be confirmed by the respective official by inscribing "Verified with originals" along with his/her name and signature on the copy of the document.

o) In cases where there arises any suspicion about the activities / life-style / income of the client. The concerned department shall also formulate a procedure for an official or a duly authorized person to undertake a visit to the residence/office of the client before accepting him as a client. This will also help in confirming that the address given by such a client is correct.

p) If account in the name of more than one person has been opened from the same address, it will ensure that such persons really reside or are related to that address. In case of a company/firm, it will ensure that the firm operates from the address given by it in the KYC form.

q) The identification procedure to be carried out while carrying out transactions for the client or when there is a doubt regarding the veracity or the adequacy of previously obtained client identification data.

r) No transaction or account-based relationship shall be undertaken without following the CDD procedure.

While dealing with clients in high risk countries where the existence / effectiveness of money laundering control is suspect, T-Cap apart from referring to the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF recommendations, published by the FATF on its website (www.fatf-gafi.org), also independently access and consider other publicly available information along with any other information which T-Cap may have access. However, this shall not preclude T-Cap from entering into legitimate transactions with clients from or situate in such high-risk countries and geographic areas or delivery of services through such high-risk countries or geographic areas. Verification of clients exposed as Politically Exposed Persons (PEP) at the time of account opening and on ongoing basis is adhered to.

Note: T-Cap should have procedures to determine whether client (existing / potential) customer is PEP. Such procedures would include seeking additional information from clients. Further approval of senior management is required for establishment business relationships with PEP and to continue the business relationship with PEP.

F. **Client identification procedure**

(a) **Identification of customer:**

T-Cap will undertake the identification of customer by collating various information as provided in detail in Annexure 1 of this policy. T-Cap will consider asking for additional information if considered necessary for identifying the customer including information related to connected / related parties.

(b) **Verification of customer:**

T-Cap will verify the customer using reliable, independent source data, documents or information (including from regulator / government website, public information, commercial databases etc.). Officially Valid Documents (OVD) as listed under Annexure 1 of this policy will be obtained for the verification of customers. T-Cap will obtain /

verify the officially valid documents provided by the customer and will maintain records of the same as required under the IFSCA guidelines.

"Officially valid document" means the passport, the driving license, proof of possession of Aadhaar number, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by Election Commission of India, , 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:

Provided that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document.

Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall be deemed to be officially valid documents:

- Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- Letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided also that where the simplified measures are applied, following documents can be used for the limited purpose of verifying the proof of address:

- Utility bill which is not more than two months old of any service provider
- Property, Municipal tax receipt, city council tax receipt or such other equivalent document;
- Bank account or Post Office savings bank account statement; etc.
- pension or family Pension Payment Orders (PPOs) issued to retired employees by
- Government Departments or Public Sector Undertakings, if they contain the address;
- Letter of allotment of accommodation from employer issued by State or Central Government Departments or Public Sector Undertakings, scheduled commercial banks, financial institutions and listed companies.

Provided also that in case the officially valid document presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, Client may submit it in such form as are issued by the Unique Identification Authority of India in the manner prescribed including redacts or blacks out Aadhaar number through appropriate mean by client when client submits a proof of possession of Aadhaar Number containing Aadhaar Number.

(c) **While on boarding the Client following shall be ensured:**

i. All officially valid documents as are specified in the KYC checklist for respective categories of customers must be received from the Client at the time of opening of account.

ii. All documents/supporting submitted by the Client are "In person verified" by the Employee of the regulated entity under his/her Name, Employee Code & Sign.

For onboarding of Foreign nationals, T-Cap will ask for the original officially valid documents for verification. In case of equivalent e-document i.e. the electronic equivalent of OVD document must be digitally signed by the issuing authority and DSC shall be in a readable format to allow verification by T-Cap. In other cases, T-Cap will obtain the certified true copy of the OVD as prescribed under the IFSCA Guidelines.

For onboarding of Indian Nationals, T-Cap may either use Video based Identification Process (V-CIP) and / or Digital KYC as mentioned in Annexure 2 of this policy.

iii. If the documentation produced by the prospective client is not in conformity with the requirements specified from time to time or if there are any inconsistencies noticed therein, no account shall be opened and matter reported to the Principal Officer immediately.

iv. As far as possible using reasonable measures, the employee dealing with the Client should ensure that the person opening the account himself is the beneficial owner or there exists sufficient documentation to corroborate his transacting on behalf of the other person, in which case appropriate due diligence would be done on the beneficial owner as well.

v. Wherever possible reasonably, efforts will be made by the employee dealing with the prospective Client to verify the details provided to him, using third party sources.

(d) Periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

(e) To put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.

(f) To obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

(g) To take reasonable measures to verify the sources of funds as well as the wealth of clients and Beneficial owners identified as PEP.

(h) T-Cap shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

- Non-Resident clients
- High Net-worth Individuals
- Trusts, Charities, NGOs and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically Exposed Persons (PEPs)

(i) Clients in high-risk countries: While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, T-Cap apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatfgafi.org)from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this does not preclude registered intermediaries from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. T-Cap shall specifically apply EDD measures including obtaining the approval of Senior Management to commence or continue the business relationship.

(j) Non face to face clients - Non face to face clients means clients who open accounts without visiting the branch/offices of the registered intermediaries or meeting the officials of the T-Cap. Video based customer identification process is treated as face-to-face onboarding of clients.

(k) Clients with dubious reputation as per public information available etc.
Explanation –
Client with Dubious Public Reputation: If a client's reputation during the opening of the account or post opening the account is known to be not good or there is uncertainty, suspicious about the integrity of that client as per the information available, then such clients are categorized as High Risk.

(l) T-Cap collects documentation requirements and other information in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by IFSCA from time to time.

Note: Any update in the information provided by the client *shall be communicated to the Regulated entity within 30 days of updation as per rule 9 of the PML Rules*

(m) T-Cap ensures that an account is not opened where T-Cap is unable to apply appropriate CDD measures. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to the intermediary is suspected to be non -genuine, or there is perceived non -cooperation of the client in providing full and complete information. T-Cap does not continue to do business with such a person and file a suspicious activity report. It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. T-Cap is

cautious to ensure that it does not return securities or money that may be from suspicious trades. However, T-Cap consults the relevant authorities in determining what action it shall take when it suspects suspicious trading.

(n) The circumstances under which the client is permitted to act on behalf of another person / entity will be determined by senior management from time to time. Accordingly the manner the account will be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details will be determined by senior management. Further the rights and responsibilities of both the persons i.e. the agent-client registered with T-Cap, as well as the person on whose behalf the agent is acting will be as laid down by senior management. Adequate verification of a person's authority to act on behalf of the client will also be carried out.

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

(p) The CDD process is necessarily revisited when there are suspicions of ML/TF.

(q) Apart from above, when establishing business relationship with a customer, an entity shall further classify the customer by assessing the following risk categories:

- risk associated with the legal form of the customer (e.g. companies having close family shareholding, partnership firm with sleeping partners, etc.);
- risk associated with the economic or personal activity of the customer (e.g. person/entity carrying out cash incentive business like restaurant business, dealing in arms, etc.);
- risk associated with the products or services used by the customer (e.g. Single premium insurance policy where the money is invested in lump sum and surrendered at the earliest opportunity, etc.)

The above-mentioned list is the minimum standard and businesses shall exercise independent judgment to ascertain whether any other set of clients shall be classified as High-Risk customer/CSC or not.

Apart from conducting the basic KYC as per the requirement of the respective business, T-Cap shall perform Enhanced Due Diligence (EDD) for its customers who are classified as High-Risk Customer and/or are covered under CSC and those clients enrolled specifically from High Risk Countries.

(r) The KYC policy covers the client identification procedure (CIP)to be carried out at different stages i.e. while establishing the intermediary –client relationship, while carrying out transactions for the client or when reporting intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

(s) T-Cap is in compliance with the following requirements while putting in place a CIP:

i. T-Cap has proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.
ii. T-Cap has obtained senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, reporting intermediary obtains senior management approval to continue the business relationship.
iii. T-Cap takes reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
iv. T-Cap identifies the client by using reliable sources including documents / information. T-Cap obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
v. The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by T-Cap in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
vi. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the senior management of T-Cap.

(t) T-Cap ensures the minimum requirements relating to KYC as specified by IFSCA from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by IFSCA from time to time, T-Cap has their own internal directives based on their experience in dealing with its clients and legal requirements as per the established practices.

(u) T-Cap conducts ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, IFSCA Act and Regulations, directives and circulars issued thereunder so that the intermediary is aware of the clients on whose behalf it is dealing.

(v) T-Cap has formulated and implemented a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

(w) T-Cap obtains the minimum information/documents from clients as stipulated in the PML Rules/ IFSCA Circulars (as amended from time to time) regarding the verification of the records of the identity of clients.

(x) There is no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by T-Cap.

(y) Reliance on Third Party for carrying out Client Due Diligence (CDD)

CDD services can be outsourced to third party. For this the third party shall mean:

i. A financial institution which is subject to and supervised by a financial regulator; or
ii. In relation to a Regulated Entity, its branches, subsidiaries, parent entity, the branches and subsidiaries of the parent entity, and other related corporations; AND
iii. Has an existing client relationship with a person whose data would be used for CDD and customer verification by T-Cap

T-Cap may rely on a third party for the purpose of –

i. Identification and verification of the identity of a client and
ii. 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. Such third party 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.

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

i. T-Cap will immediately obtains necessary information of such client due diligence carried out by the third party;
ii. T-Cap takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
iii. T-Cap will be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
iv. The third party is not based in a country or jurisdiction assessed as high risk;
v. No Regulated Entity shall rely on a third party to conduct ongoing monitoring of business relations with customers;
vi. No Regulated Entity shall rely on a third party specifically precluded by the Authority from relying upon;
vii. The Regulated Entity shall document the basis for its satisfaction that the requirements under sub-clause (iii) above, have been met;
viii. The reliance on Third Party shall also be subject to the conditions that are specified in rule 9 (2) of the Rules and shall be in accordance with the regulations and circulars/guidelines issued by Authority from time to time.
ix. T-Cap is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

(z) Use of Business Facilitator

T-Cap may also use the services of business facilitators from various jurisdictions for verifying the information/OVD provided by the customer ensuring secrecy and data protection. T-Cap will ensure that no business facilitators is from jurisdictions which

has been identified as 'High Risk Jurisdictions' subject to a 'Call for Action' in public statement of FATF. T-Cap will maintain the complete details of services taken from business facilitators.

G. Monitoring of Transactions

a) Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. T-Cap has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities.

b) T-Cap pays special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. T-Cap carries specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/office records / memorandums / clarifications sought pertaining to such transactions and purpose thereof is examined carefully and findings is recorded in writing. Further such findings, records and related documents is made available to auditors and also to IFSCA/stock exchanges/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required.

c) T-Cap applies client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring is aligned with the risk category of the client.

d) T-Cap ensures a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions is regularly reported to the higher authorities.

e) The compliance cell of T-Cap to randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

Periodic Updation:

T-Cap will perform periodic updation of CDD in following manner:

- Annually – for high risk customers
- Once in every three years – for medium risk customers
- Once in every five years – for low risk customers

T-Cap will also undertake review both periodically and at appropriate times, when:

(i) it changes its CDD documentation requirements;
(ii) an unusual transaction with the customer is expected to take place;
(iii) there is a material change in the business relationship with the customer; or
(iv) there is a material change in the nature or ownership of the customer

(a) **Individual Customers:**
No change in CDD – self declaration will be obtained through mobile number registered or digital channels

Change in Address - self-declaration of the new address will be obtained from the customer through customer's email-id registered or digital channels and is verified within two months. Copy of proof of address is obtained at the time of periodic update.

(b) **Other than Individual:**
No change in CDD – Self declaration through email id registered, digital channels, letter duly signed by authorize official and requisite resolutions in this regard is obtained from the customer
Change in CDD Information – Fresh CDD process is undertaken

H. Suspicious Transaction Monitoring and Reporting

(a) T-Cap ensures that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, T-Cap is guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

Steps to determine suspicious transactions:

T-Cap will follow the above-mentioned steps to determine suspicious transactions:

i. Detecting red flags for suspicious transactions – based on indicators such as complex and unusual transactions, unusual customer behaviour, countries with high-risk jurisdiction, etc.
ii. Inquiring the customers on the transactions highlighted through red flags – care should be taken not to tip off the customer
iii. Reviewing the customer records with respect to the transactions which includes customer's occupation, transaction history, risk profile, etc.
iv. Evaluating the above information to conclude a suspicious transaction and report it to FIU-IND.

(b) 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:

i. Clients whose identity verification seems difficult or clients that appear not to cooperate;
ii. Asset management services for clients where the source of the funds is not clear or not in keeping with clients' apparent standing /business activity;
iii. Clients based in high risk jurisdictions;
iv. Substantial increases in business without apparent cause;
v. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
vi. Attempted transfer of investment proceeds to apparently unrelated third parties;
vii. Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services.

(c) Any suspicious transaction is immediately notified to the Designated / Principal Officer at T-Cap. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall not be told of the report/ suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated Director/ Principal Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

(d) 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. It is clarified that T-Cap reports all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

(e) Clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC' as specified in this policy. Such clients are subject to appropriate counter measures. These measures include further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

I. Reporting to Financial Intelligence Unit-India

a) In terms of the PML Rules, we have 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, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone: 91-11-23314429, 2331445991-11-23319793(Helpdesk)
Email: helpdesk@fiuindia.gov.in
(For FINnet and general queries) ctrcell@fiuindia.gov.in
(For Regulated Entity / Principal Officer registration related queries) complaints@fiuindia.gov.in Website: http://fiuindia.gov.in

b) T-Cap ensures all the reporting requirements and formats that are available on the website of FIU –IND under the Section Obligation of Regulated Entity – Furnishing Information-Reporting Format (https://fiuindia.gov.in/files/downloads/Filing_Information.html).

c) T-Cap shall ensure the related hardware and technical requirement for preparing reports, the related data files and data structures required for reporting purpose. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, T-Cap adhere to the following:

i. The Cash Transaction Report (CTR) (wherever applicable) for each month will be submitted to FIU-IND by 15th of the succeeding month.

ii. The Suspicious Transaction Report (STR) will be submitted immediately of arriving at conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer will record his reasons for treating any transaction or a series of transactions as suspicious. T-Cap will ensure that there is no undue delay in arriving at such a conclusion.

iii. The Principal Officer will be responsible for timely submission of STR to FIU-IND;

iv. Utmost confidentiality will be maintained in filing of CTR, STR and NTR to FIU IND.

v. No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/non-profit organization transactions to be reported.

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

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, T-Cap will file STR if we have reasonable grounds to believe that the transactions involve proceeds of crime.

The "proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

Confidentiality requirement does not inhibit information sharing among entities in the group.

J. Record Management

Information to be maintained

T-Cap maintains and preserves the following information in respect of transactions:

a. A copy of all documents and information collected from the customers relating to CDD
b. Records of customer business relationships which includes information relating to a customer's account, adequate records of transactions to enable standalone transactions to be reconstructed, internal findings and analysis relating to a business transaction of unusual or suspicious nature and whether or not it results in a Suspicious Transactions Report (STR)

c. Notification to Principal officer by any employee of any known or suspected ML/TF risks
d. STRs and any relevant supporting documents and information, including internal findings and analysis
e. Any communications to FIU-IND
f. Maintenance of training records
g. Outcome of business risk assessment and its usage for CRA
h. Risk assessment of each customer
i. Determination of risk rating of each customer
j. Any other matter expressly required to record and maintain

Record Keeping

a. T-Cap ensures compliance with the record keeping requirements contained in the IFSCA Act, Rules and Regulations made thereunder, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

b. T-Cap maintains such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

c. In case of any suspected laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, T-Cap shall retain the following information for the accounts of their clients in order to maintain a satisfactory audit trail: i. the beneficial owner of the account; ii. the volume of the funds flowing through the account; and iii. for selected transactions:
   - the origin of the funds
   - the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
   - the identity of the person undertaking the transaction;
   - the destination of the funds;
   - the form of instruction and authority.

d. T-Cap ensures that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the IFSCA Act, Rules and Regulations framed thereunder PMLA, other relevant legislations, Rules and Regulations or Exchange byelaws or circulars.

e. Where the T-Cap does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which T-Cap shall close the account of the clients after giving due notice to the client.

   Explanation: For this purpose, the expression “records of the identity of clients” shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

K. Retention of Records

a) T-Cap has taken appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities

b) T-Cap has formulated and implemented the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of six years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

c) In situations where the records relate to on-going investigations or transactions which have been the subject of suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

d) T-Cap maintains and preserves the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU –IND, as required under Rules 7 and 8 of the PML Rules, for a period of six years from the date of the end of transaction between the client and the intermediary.

L. List of Designated Individuals/ Entities

a) The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. T-Cap uses such lists of designated individuals/terrorists, as and when communicated by IFSCA.

b) All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by IFSCA from time to time T-Cap uses for compliance.

c) An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) is accessed at its website at https://press.un.org/en/content/press-release. The details of the 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://www.un.org/securitycouncil/sanctions/1267/press-releases.
   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

d) T-Cap ensures that accounts are not opened in the name of anyone whose name appears in said list. T-Cap 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.

e) T-Cap maintains an updated designated lists through the system and run a check on the given parameters on a regular basis to verify whether the designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

f) T-Cap shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements

g) T-Cap files a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

h) Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 01123092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

i) A copy of the communication shall also be sent to the State Nodal officer/ UAPA, IFSCA and FIU-IND, without delay.

M. Procedure for freezing funds, financial assets or economic resources or related services

a) T-Cap ensures that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, T-Cap do not have any accounts 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).

In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1- Link: https://www.mha.gov.in/sites/default/files/202305/ProcedureImplementationSection51A_04052023.pdf) for strict compliance.

b) 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

N. Jurisdictions that do not or insufficiently apply the FATF Recommendations

a) FATF Secretariat after conclusion of each of it's plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by IFSCA from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, is considered by T-Cap.

b) T-Cap takes into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements. However, it shall be noted that the regulated entities are not precluded from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statements.

O. Designation of officers for ensuring compliance with provisions of PMLA

Appointment of a Principal Officer:

T-Cap has appointed Compliance Officer to act as the Principal officer to oversee the reporting requirements as prescribed under the IFSCA Guidelines.

T-Cap shall ensure to properly discharge their legal obligations to report suspicious transactions to the authorities, for which 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. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by a registered intermediary;

Provided that such officer shall be an officer at the management level.

Responsibilities of Principal Officer:

- carrying out, or overseeing the carrying out of, ongoing monitoring of business relations for compliance with the IFSCA Guidelines;
- promoting compliance of the IFSCA Guidelines and taking overall charge of all AML/CFT matters within the organisation;
- informing employees, officers and representatives promptly of regulatory changes;
- ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
- reporting or overseeing the reporting of suspicious transactions;
- advising and training employees, officers and representatives on developing and implementing internal policies, procedures and controls on AML/CFT;
- reporting to Senior Management on the outcome of reviews of the Regulated Entity's compliance and risk assessment procedures; and
- responsibility with respect to timely submission of STR to FIU-IND
- reporting regularly on key AML/CFT risk management and control issues, and any necessary
- remedial actions, arising from audit, inspection & compliance reviews to the Senior Management

Appointment of a Designated Director:

In addition to the existing requirement of designation of a Principal Officer, T-Cap has designated a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

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

Rules and includes –

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

Accordingly, T-Cap has appointed Principal Officer of the Company to act as the Designated Director for overseeing the overall compliance requirements with the IFSCA Guidelines, PML Act and rules thereto.

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

T-Cap has communicated and will update in case of any changes, the details of the Designated Director, such as, name designation and address to the Office of the Director, FIU –IND.

P. Hiring and Training of Employees and Investor Education and Audit Function

Hiring of Employees:

T-Cap have adequate screening procedures in place to ensure high standards when hiring employees. T-Cap have system in place to identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

Training of Employees:

T-Cap has an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements covers specific focuses for frontline staff, back-office staff, compliance staff, risk management staff and staff dealing with new clients. T-Cap ensures that concerned fully understands 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.

Investor Education:

For implementation of AML/CFT measures T-Cap demands certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the client with regard to the motive and purpose of collecting such information. T-Cap sensitize their clients about these requirements as the ones emanating from AML and CFT framework. T-Cap will prepare specific literature/ pamphlets etc. if required, so as to educate the client of the objectives of the AML/CFT programme.

Audit Function:

T-Cap has developed an independent audit function to assess the effectiveness of this policy and periodic audits are undertaken at regular intervals as part of this audit function.

Q. Sharing of KYC information pertaining to Indian Resident (Natural and Legal Entities) with Central KYC Records Registry (CKYCR):

T-Cap will have adequate system in place to upload customer's KYC records on CKYCR, whenever applicable for the IFSCA regulated entities. Such sharing of KYC information will be applicable for the customers of Indian nationality within 10 days of commencement of an account-based relationship with the customer and in the form prescribed under Central KYC Registry Operating Guidelines 2016, released by Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI).

12. **Policy Review**

This Policy shall be reviewed annually or as and when there are any regulatory changes introduced or as and when it is found necessary to change the Policy due to business / industry needs. The Policy shall be placed before the Directors of the T-Cap for approval.

13. **Deviation to Framework**

Major deviations to the Policy shall be approved by the Board; all other deviations shall be approved by respective entities Designated Director and Principal officer.

14. **Power to Remove Difficulties**

In order to remove any difficulties in the application or interpretation of this Policy, the Principal Officer or Compliance Officer shall have the power to issue clarifications.

15. **Effective Date**

This policy will be effective from April 2026.

IMPORTANT INFORMATION

If at any point a conflict of interpretation/ information between this Policy and any Regulations, Rules, Guidelines, Notifications, Clarifications, Circulars, Master Circulars applicable to T-Cap issued by the IFSCA (or any other regulator then applicable to T-Cap) arises, then interpretation of such Regulations, Rules, Guidelines, Notification, Clarifications, Circulars, Master circulars issued by IFSCA or such other regulator shall prevail over this Policy.

Annexure 1

Checklist for Customers

Following information / documents are required for undertaking the customer due diligence:

Information / Documents required for Identification / Verification of Customers (Only for Individuals)

Sr No.	Particulars of Information	Details / Official valid documents required
1	Personal Details (Information)	• Full Name • Date of Birth • Permanent address • Current residential address (other than a post office box address) • Gender • Nationality • PAN (for Indian Nationals)
2	Proof of Identity and Address (Documents)	• Copy of Passport / Voter-Id / Driving License / Aadhar / Letter issued by National Population Register (For Indian Nationals) • Certified true copy[1] of National identity card (including passport) and voter identification card issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national (For Foreign Nationals) ***Note:*** *In case the permanent address and current residential address are different, two different OVDs shall be given to verify both the address details.* *If the above documents are not available, kindly refer documents mentioned under simplified measures according to the risk rating of the customers.*
3	Contact Details	• Mobile Number / Phone Number • Email Id • Fax details, if any
4	Occupational Details	• Service (Private Sector, Public Sector, Government Sector) • Business • Others

[1]Obtaining a certified copy shall mean comparing the officially valid document provided by the customer with copy thereof and recording the same as "true copy" by the authorized officer of the Regulated Entity (RE). In case the customer is unable to produce, or it might not be possible for customer to submit original documents for verification (e.g., in situations where Regulated Entity has no physical contact with the customer, or the onboarding of customer is done through non-face to face mode); a Regulated Entity should obtain a copy of the OVD that is certified to be a 'true copy' and such certification may be carried out by any one of the following:

- authorized officials of a bank located in a Financial Action Task Force (FATF) compliant jurisdiction with whom the individual has banking relationship
- branches of overseas banks with whom Indian banks have relationships
- Notary Public abroad
- Court Magistrate (outside India)
- Judge (outside India)
- Certified public or professional accountant (outside India)
- Lawyer (outside India)
- Indian Embassy/Consulate General in the country of which the non-resident individual is a citizen

Any other authority as may be specified by the IFSCA.

Information / Documents required for Identification / Verification of Customers (Only for Legal Arrangement)

Sr No.	Particulars of Information	Details / Official valid documents required
1	Company Details	• Entity Name • Legal form of the entity • Date of Incorporation • Place of Incorporation • Nature of Business • Corporate Identification Number / LLPIN / Equivalent Identification number • PAN or equivalent number prevalent in the home jurisdiction of the company
2	Proof of Identity and Address	• Certificate of Incorporation / Registration Certificate • Memorandum and Articles of Association / Charter Documents Partnership Deed / LLP Deed / Trust Deed • PAN or equivalent document prevalent in the home jurisdiction of the company • Resolution passed by Board or Partners or Trustees / Power of Attorney *(Please note that for the entities incorporated in foreign jurisdiction, the above documents shall be certified to be a true copy)*
3	Contact Details of Authorised Signatory	• Mobile Number / Phone Number • Email Id • Fax details, if any
4	Any Other Information	Official Valid Documents (please refer point 2 of individuals) required for following persons: • Beneficial owners • Directors / authorised officials who shall act or is appointed to act on behalf of company or Partners / Directors / authorised officials who shall act or are appointed to act on behalf of firm / LLP, as the case may be

Additional Points for clarification:

Simplified Measures –

In case of low-risk customers, following documents are also acceptable for verifying the identity of the customers and such documents will be deemed to be OVD:

(i) identity card with applicant's photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
(ii) letter issued by a gazetted officer, with a duly attested photograph of the person.

In case of low-risk customers, the following documents would also be acceptable for the limited purpose of verifying the proof of address of the customer.

Further, the following documents will also be temporarily acceptable in case of high risk and medium risk customers for the limited purpose of verifying the address proof. However, such medium risk and high-risk customers shall submit updated OVD (please refer point 2 of individuals) or their equivalent e-documents thereof with current address within a period of three months of submitting the following documents:

(i) Utility Bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill)
(ii) Property or Municipal tax receipt, or such equivalent document
(iii) Post Office savings bank account statement or statement of a bank account including of a foreign bank
(iv) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
(v) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation
(vi) For Foreign Nationals - documents issued by the Government departments of foreign jurisdictions or letter issued by the Foreign Embassy or Mission in India shall be deemed to be OVD for limited purpose of address proof.

Annexure 2

Video based Customer Identification and Digital KYC

Part A - V-CIP Process for Onboarding of Indian Nationals

Video based Customer Identification Process or "V-CIP" means an alternate method of customer identification with facial recognition and customer due diligence, by an authorised official of the Regulated Entity, by undertaking seamless, secure, live, informed & consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process.

1.1. T-Cap IFSC may undertake V-CIP to carry out:

(a) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons.

(b) Updation / Periodic updation of KYC for eligible customers.

1.2. Opting to undertake V-CIP, shall adhere to the following minimum standards:

V-CIP Infrastructure

(i) T-Cap IFSC shall comply with the minimum baseline cyber security and resilience framework as may be specified, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process should be compliant with the standards as may be specified.

(ii) Ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.

(iii) T-Cap IFSC shall also ensure that all such data including video recordings are transferred to the server(s)/cloud server owned or taken on lease by the Regulated Entity or its Financial Group, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the T-Cap IFSC.

(iv) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(v) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(vi) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate

responsibility of any customer identification rests with the T-Cap IFSC. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

(vii) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

(viii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration Testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as may be specified. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(ix) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

V-CIP Procedure

(i) Formulate a clear workflow and standard operating procedure for V- CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the entity specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(ii) If there is a disruption in the V-CIP procedure, the same should be aborted and a fresh session initiated.

(iii) The sequence and/or type of questions, including those indicating the liveness of the interaction during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

(iv) Any prompting, observed at the end of customer shall lead to rejection of the account opening process.

(v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of workflow.

(vi) The authorised official performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:
   (a) Offline Verification of Aadhaar for identification;
   (b) KYC records downloaded from CKYCR using the KYC identifier provided by the customer;
   (c) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.

(d) Biometric based e-KYC authentication, including Aadhaar Face Authentication can be done.
(e) OTP based Aadhaar e-KYC authentication

(vii) Ensure to redact or blackout the Aadhaar number in the manner as provided under Part B of Annexure 2.

(viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three days from the date of carrying out V-CIP.

(ix) Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document; if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, T-Cap IFSC shall ensure that no incremental risk is added due to this.

(x) If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.

(xi) T-Cap IFSC shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi-locker.

(xii) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(xiii) The authorised official shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

(xiv) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.

(xv) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the T-Cap IFSC.

V-CIP Records and Data Management

(a) The entire data and recordings of V-CIP shall be stored in a system / systems located in the territory of India. T-Cap IFSC shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in these Guidelines, shall also be applicable for V- CIP.

(b) The activity- log along with the credentials of the authorised person performing the V-CIP shall be preserved.

Additional conditions or requirements for Onboarding Non-Resident Indian (NRI) Customers (classified as low-risk) through V-CIP.

i. The Regulated Entities may onboard customers, who are Non- Resident Indian ('NRI Customers'), through V-CIP to carry out:

a) CDD in case of on-boarding of new customers such as individual, proprietor in case of proprietorship, authorised signatories and Beneficial Owners (BOs) in case of customers which are non-natural persons and other connected parties appointed to act on behalf of the customer;

b) Updation/Periodic updation of KYC.

For the purposes of this part, the term "NRI customer" shall refer to a Non-Resident Indian who has been classified as a low-risk customer, by the Regulated Entity in accordance with these Guidelines, and resides in any of the following jurisdictions:

a)United States of America;
b)Japan;
c)South Korea;
d)United Kingdom excluding British Overseas Territories;
e)Canada;
f)UAE;
g)Singapore;
h)Australia;
i)European Union excluding Croatia

For the avoidance of doubt, it is hereby clarified that the T-Cap shall undertake V-CIP only for NRI customers residing in any of the above specified jurisdictions and submits valid proof of current address to that effect.

While undertaking the V-CIP for onboarding the NRI customers, T-Cap shall ensure that the IP address emanates from the jurisdiction specified in the current address proof submitted.

T-Cap shall also capture the bank account details, maintained by NRI Customer with any bank in the jurisdiction specified in Explanation 1 above, for the purpose of verification of the current address.

Upon verification of the proof of identity of the NRI Customer, in cases where current address of NRI customer cannot be verified from reliable/issuing authority sources, the Regulated Entity shall open the account of the customer in the debit freeze / inactive mode; and shall communicate such customer the manner of activation of debit freeze / inactive account.

The said debit freeze / inactive account of the NRI Customer shall be made operational only upon the receipt and verification of first credit from the bank account provided

by such customer as proof of current address at the time of V-CIP onboarding process

Part B - Digital KYC Process for Indian Nationals

"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification[2] cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Regulated Entity as per the provisions contained in the Act.

1.1. For undertaking CDD of Indian nationals, obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where: -

(i) the customer decides to submit his Aadhaar number voluntarily to a bank or any Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(bb) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of the customer's identity and address; and

(b) the Permanent Account Number or the equivalent e-document thereof, as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof, as may be required by the entity:

Provided that where the customer has submitted,

(i) Aadhaar number under Clause (a) above, to a bank or a Regulated Entity notified under first proviso to sub-section (1) of section 11A of the Act, such bank or Regulated Entity shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Regulated Entity.

(ii) proof of possession of Aadhaar under sub-clause (aa) above, where offline verification can be carried out, carry out offline verification.

(iii) an equivalent e-document of any OVD, verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued thereunder and take

[2] *As per the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 "offline verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations.*

a live photo as specified under digital KYC Process as specified under Annexure I of Rules[3].

(iv) any OVD or proof of possession of Aadhaar number under (a)(i)(bb) above where offline verification cannot be carried out, carry out verification through digital KYC Process as specified under Annexure I of Rules.

Provided that for a period not beyond such date as may be notified by the Government, instead of carrying out digital KYC, obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

***Explanation I*:** Where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means.

***Explanation II*:** Biometric based e-KYC authentication can be done by authorised official of the T-Cap IFSC/business facilitators.

***Explanation III*:** The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Annexure I of PML (Maintenance of Records) Rules 2005

Digital KYC Process

A. The reporting entities shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated Application of the Reporting Entities.

B. The access of the Application shall be controlled by the Reporting Entities and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Reporting Entities to its authorized officials.

C. The client, for the purpose of KYC, shall visit the location of the authorized official of the Regulated Entity or vice-versa. The original Officially Valid Document (OVD) shall be in possession of the client.

D. The Regulated Entity must ensure that the Live photograph of the client is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Regulated Entity shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Reporting Entities) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the client.

E. The Application of the Reporting Entities shall have the feature that only live photograph of the client is captured and no printed or video-graphed photograph of the client is captured. The background behind the client while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the client.

[3] *Rules refers to PML (Maintenance of Records) Rules 2005*

F. Similarly, the live photograph of the original officially valid document or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

G. The live photograph of the client and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the client. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to client's own mobile number. Upon successful validation of the OTP, it will be treated as client signature on CAF. However, if the client does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Regulated Entity shall not be used for client signature. The Regulated Entity must check that the mobile number used in client signature shall not be the mobile number of the authorized officer.

J. The authorized officer shall provide a declaration about the capturing of the live photograph of client and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Regulated Entity. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the Regulated Entity, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to client for future reference.

L. The authorized officer of the Regulated Entity shall check and verify that: -

(i) information available in the picture of document is matching with the information entered by authorized officer in CAF.

(ii) live photograph of the client matches with the photo available in the document.; and

(iii) all of the necessary details in CAF including mandatory field are filled properly.;

On Successful verification, the CAF shall be digitally signed by authorized representative of the Regulated Entity who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

ANNEXURE 3

PARAMETERS FOR SUSPICIOUS TRANSACTIONS REPORTING

SN	Reason Code	Particulars	Description	Threshold value
1	CV 3	KYC failure	Where KYC has failed and has not been regularized over a rolling period of 3 months. KYC under process for long period KYC in process status for more than 3 months.	
2	CV 9	Existing Customer behavior/ Changes to demographics	For open ended schemes, if the number of transactions is > 5 times than the preceding year and value of transaction is > 5 times the average value of the preceding year, then it would be reported	
3	STR 1	Use of Demand Drafts for investments	Demand drafts used for payment of draw down amount.	
4	STR 3	PEP matches	Investors identified as PEP at the time of onboarding or becomes PEP subsequently	
5	STR 4	Matches with World Compliance data	Transactions which have relevant matches in the AML screening check	
6	STR 5	FATF banned countries	Transactions which are received from FATF jurisdictions	
7	STR 6	WMD Proliferation Financing	Transactions linked to entities involved in Weapons of Mass Destruction per UNSC resolutions.	
8	TM 10	Transactions in folio operated by POA holders	Transactions above a certain threshold value where the folios are operated by POA holders. PMS investors, Channels, Banks may be excluded. Threshold is to be decided by the FMEs.	

SN	Reason Code	Particulars	Description	Threshold value
9	TM 2	Use of different accounts by client alternatively	Individuals: a. Individual investing via more than 5 bank accounts during his / her tenure as an investor or the last one year whichever is lesser or b. Registers more than 5 bank accounts during his / her tenure as an investor. Non-Individuals: a. Non-individual investors investing in any scheme via more than 10 bank accounts during its tenure as an investor or the one year whichever is lesser b. Registers more than 10 bank accounts during its tenure as an investor.	
10	TM 3	Short period opposite transactions	Short Period Opposite Transactions: Two opposite transactions in a folio within a scheme in a rolling period of 14 calendar days, except transactions in liquid/Ultra Short-Term Debt funds. Purchases, redemptions and switches are to be considered, to consider the period of 14 days from initial purchase till date of redemption. Only for retail schemes: Individuals: Threshold amount of at least one of the transactions will be USD 30,000 and above For Non individuals: Threshold amount of at least one of the transactions will be USD 75,000 and above (All systematic transactions are excluded)	
11	TM 4	Non-Financial Activity in Accounts.	1. Change of address or change in bank mandate during a rolling 12-month period, where: a. Changes to bank mandate are executed by individual investors (including HUF) involving more than three different bank accounts (account numbers are different). These changes are over and above registered bank accounts OR b. Changes to bank mandate are executed by non-individual investors involving more than five different bank accounts (account numbers are different). These changes are over and above registered bank accounts OR c. Changes to address are executed by any	

SN	Reason Code	Particulars	Description	Threshold value
			investor (individual and non-individual) involving more than 3 different addresses	
12	TM 5	Investment vis-à-vis the declared income as per last available / any revised KYC application form	a) Single purchase transaction of an Individual Investor in a Financial year is 10 or more times of the upper band * of the annual income specified by that investor in the KYC form.\ b) Cumulative purchase transactions (cost value) by an Individual Investor in a Financial year is 20 or more times of the upper band* of the annual income specified by that investor in the KYC form. *However, in case of highest income bracket where the upper income band is not mentioned then the lower band shall be considered. Special emphasis must be laid by Fund Houses on investors who are minors/ students/ housewives/ retired persons / forex dealers / persons who have categorized themselves as "others")	
13	TM 6	Change in bank mandate used for debit for Systematic Investment Plan investments SIP	Where an investor uses multiple bank accounts to debit for SIP. investments i.e. more than 3 in one rolling year and the amount of investment exceeds USD 3,000 in such a period	
14	TM 7	Multiple Joint holders	Where one investor (identified by PAN) is investing as a joint holder (2nd or 3rd) with 5 or more different first unit holders (also identified by PAN) at any point in time.	
15	TM 9	Short Term redemption to a different bank mandate	Investor(s) made purchase from a given bank mandate and made a short-term redemption request (14 days or less) with a different bank mandate.	

ANNEXURE 4

RISK RATING PARAMETERS FOR CUSTOMERS

Risk Parameter	Type	Associated Rating*	Weightage % (should add up to 100)
Tax Status	Bank/Financial institution	0	**15**
	Listed Company & associate companies	0	
	Public Sector undertakings	0	
	Provident Fund/EPF	0	
	Superannuation fund	0	
	Gratuity Fund	0	
	Pension Fund	0	
	NPS trust	0	
	Foreign Inst Investor	0	
	Foreign Portfolio Investor – Category I	1	
	Foreign Portfolio Investor – Category II	3	
	Foreign Portfolio Investor – Category III	5	
	Individual - Resident and Non Resident	1	
	On Behalf of Minor	1	
	HUF	1	
	Sole proprietorship	1	
	Insurance Companies	2	
	Partnership	3	
	Body Corporate	4	
	Society	4	
	AOP/BOI	5	
	Limited Liability Partnership	5	
	Trust (Others)	7	
	Private Family Trust	8	
	Charitable Trust / NPO	10	
	Others / Not Declared	10	
	Bank/Financial institution, Listed Company & associate companies, Public Sector undertakings, Provident Fund/EPF, Superannuation fund, Gratuity Fund, Pension Fund, NPS trust	0	
Occupation	Service (private, public, government)	1	**15**
	Retired	5	
	Agriculture	7	
	Housewife	7	
	Student	7	

	Business – 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, Transport Operators, Auto dealers (used / reconditioned vehicles / motor cycles), Scrap metal dealers, Import / Export, Gas Station.	10	
	In case of Professional / Self Employer, Other Business, Manufacturing & Service Sector other than the one listed above, the risk rating will be as below		
	Investment Above 8 times of income Range	7	
	Investment - Above 5 and upto 8 times of income range	5	
	Investment - Above 4 and upto 5 times of income range	3	
	Investment - 1 to 3 times of Income Range	2	
	Others	10	
	Not specified	10	
	Unknown	10	
PEP Status *(based on self-declaration)*	No	0	**15**
	Yes / RPEP	10	
KYC Documents Verification	No	10	**10**
	Under Process	8	
	Yes	0	
Commitment Amount	Upto 250000 USD	1	**10**
	Above 250000 and upto 600000 USD	2	
	Above 600000 USD upto 1200000 USD	3	
	Above 1200000 USD upto 3000000 USD	4	
	Above 3000000 USD upto 6000000 USD	5	
	Above 6000000 USD	6	
Country of Residence	North Korea	10	**15**
	Iran	10	

	Balkans, Belarus, Burma, Burundi, Cote D'Ivoire (Ivory Coast), Central African Republic, Cuba, Democratic Republic of Congo, Lebanon, Libya, Somalia, Iraq, Liberia, Sudan (including south Sudan), Palestine, Syria, Yemen, Venezuela, Ukraine and Zimbabwe / FATF countries	7	
	India	0	
	Others	1	
Part of Watchlist / Sanction lists or any negative news	No	0	**20**
	Yes	10	

*(0 to 10, where 0 is the lowest and 10 is the highest)

Risk Rating	
Upto 1.5	Low
Above 1.5 upto 2.5	Medium
Above 2.5	High

ANNEXURE 5

RED FLAG INDICATORS FOR SUSPICIOUS TRANSACTIONS

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
1	CVI: Verification of Client credentials	Fake / improper documents and information is provided for KYC and any repository of KYC reject such applications.	Any instances of improper documentation would be brought to the notice of the AMC
2	CV 2: Client Address Verification	Any account opening communications where they are returned undelivered, especially with reasons like address not found, person does not exist, incomplete address, etc.	RUD tracker for bounced mails & physical dispatch (if any) will be maintained and shared with FME
3	CV 3: Status of KYC Process	KYC could not be completed even after EDD in cases where KYC status of a person could not be determined within 3 months.	Will be flagged as part of the daily report being shared
4	CV 4: Establishing UBO	UBO is not established / is a sleeping partner / difficult to be established / where there is non-cooperation in furnishing UBO details / matches found in the watch lists	If any such instance found then to be included in RFI monthly report
5	CV 5: Ongoing KYC	Unusual transactions by the investors such as multiple updation in the KYC information / documentation at the time of onboarding / KYC updation.	FME actionable. Since documents flow from FME to CAMS, AMC is better positioned to know if multiple KYC documentation was submitted by investor
6	CV 6: Existing Customer Behaviour/ Changes to demographics	Change in Authorized Signatories - Negative credential of such persons and/or frequency of such changes	Ascent India will screen the new ASL (if received) and update FME on the outcome
7	CV 7: Existing Customer behaviour/ Changes to demographics	Investors identified as PEP at the time of onboarding or becomes PEP subsequently	Reverse screening checks being implemented. So subsequent alerts (if any) will also be intimated to FME.
8	CV 8: Existing Customer behaviour/ Changes to demographics	Investors change address to FATF designated Non-Cooperative Countries and Territories/ drug trafficking sensitive countries/ High Risk and other monitored jurisdictions	If any such instance found then to be included in RFI monthly report
9	CV 9: Existing Customer behaviour/ Changes to demographics	Sudden increase in number of transactions in a folio / set of folios of same customer. If the number of transactions in a folio / set of folios is 5 times the average number of transactions coupled with a value threshold of the same set in the preceding 1 year	Not applicable for close ended schemes. For open ended schemes, if the number of transactions is >5 times than the preceding

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
			year and value of transaction is > 5 times the average value of the preceding year, then it would be reported
10	CV 10: Suspicious Attempted Transactions	Prospective clients who do not invest after being informed of the KYC requirements or do not co-operate/ insist that KYC norms be relaxed/ circumvented for accommodating their transactions.	FME actionable
11	CV 11: Suspicious Attempted Transactions	If identity of the client matches with the identity of a person having known criminal background or certain adverse comments are found for that respective investor or is banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.	Covered as part of AML screening.
12	Noncompliance of KYC prior to redemption	Any unjustified / unreasonable stand from the customer in terms of not cooperating to provide KYC information prior to redemption.	FME actionable
13	TM 1: Activity in Accounts - Unusual activity compared to past transactions:	Where one single subscription transaction (5 or more times for Retail schemes, 10 or more times for Restricted and Venture Capital schemes) is greater than the average of all PRIOR subscription transactions by one investor during the last 3 years (b) Dividend Reinvestment, switches and systematic transaction values should be excluded.	Already covered under STR for open ended schemes
14	TM 2: Use of different accounts by client alternatively. Individuals and Non-Individuals	Individuals: a. Individual investing via more than 5 bank accounts during his / her tenure as an investor or the last one year whichever is lesser or b. Registers more than 5 bank accounts during his / her tenure as an investor. Non-Individuals: a. Non-individual investors investing in any scheme via more than 10 bank accounts during its tenure as an investor or the one year whichever is lesser b. Registers more than 10 bank accounts during its tenure as an investor.	Already covered under STR

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
15	TM 3: Short Period Opposite Transactions:	Short Period Opposite Transactions: Two opposite transactions in a folio within a scheme in a rolling period of 14 calendar days, except transactions in liquid/Ultra Short-Term Debt funds. Purchases, redemptions and switches are to be considered, to consider the period of 14 days from initial purchase till date of redemption. Only for retail schemes: Individuals: Threshold amount of at least one of the transactions will be USD 30,000 and above For Non individuals: Threshold amount of at least one of the transactions will be USD 75,000 and above (All systematic transactions are excluded)	Applicable only for open ended schemes /Retail schemes and is part of the STR
16	TM 4: Non-Financial Activity in Accounts	Non-Financial Activity in Accounts: Change of address or change in bank mandate during a rolling 12-month period, where: a. Changes to bank mandate are executed by individual investors (including HUF) involving more than three different bank accounts (account numbers are different). These changes are over and above registered bank accounts OR b. Changes to bank mandate are executed by non-individual investors involving more than five different bank accounts (account numbers are different). These changes are over and above registered bank accounts OR c. Changes to address are executed by any investor (individual and non-individual) involving more than three different addresses.	Already covered as part of STR

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
17	TM 5: Investment vis-à-vis declared income as per last available / any revised KYC application form:	a) Single purchase transaction of an Individual Investor in a Financial year is 10 or more times of the upper band * of the annual income specified by that investor in the KYC form. b) Cumulative purchase transactions (cost value) by an Individual Investor in a Financial year is 20 or more times of the upper band* of the annual income specified by that investor in the KYC form. *However, in case of highest income bracket where the upper income band is not mentioned then the lower band shall be considered. Special emphasis must be laid by Fund Houses on investors who are minors/ students/ housewives/ retired persons/forex dealers / persons who have categorized themselves as "others")	Will be covered as part of STR
18	TM 6: Change in bank mandate used for debit for Systematic Investment Plan investments SIP	Where an investor uses multiple bank accounts to debit for SIP. investments i.e. more than 3 in one rolling year and the amount of investment exceeds USD 3,000 in such a period	Covered as part of STR
19	TM 7: Multiple Joint holders	Where one investor is investing as a joint holder with 5 or more different first unit holders at any point in time	Covered as part of STR

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
20	TM 8: Transaction of Clients in special categories and high risk category clients	All transactions or transactions over USD. X along with certain other factors like income, profession, country where he/ she/ the entity resides etc., maybe monitored for such clients. Threshold is to be decided by the FMEs.	Firstly, the said RFI is applicable only for High Risk Investor. **Proposed Threshold:** Amount: USD 500,000 Income Range: Investment Above 8 times of income Range Profession: Business – 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, Transport Operators, Auto dealers (used / reconditioned vehicles / motor cycles), Scrap metal dealers, Import / Export, Gas Station. Country of residency: FATF Grey Listed Countries Is part of STR parameter.
21	TM 9: Short Term redemption to a different bank mandate	Investors(s) made purchase from a given bank mandate and made a short-term redemption request (14 days or less) with a different bank mandate.	Applicable only for Open ended and retail schemes. Shall be included as part of STR
22	TM 10: Transactions in folio operated by POA holders	Transactions above a certain threshold value where the folios are operated by POA holders. PMS investors, Channels, Banks may be excluded. Threshold is to be decided by the FMEs.	Will be added as a STR criteria and tracked Suggested threshold USD 500,000
23	TM 11: WMD/UNSC Matches	Matches with UNSC sanctions or WMD proliferation lists.	overed as part of AML screening; report NTR if applicable
24	LQI: Customer is being investigated for criminal offences	Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences	Covered as part of AML screening.

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
	High-Risk Jurisdiction Exposure	Increased transactions from high-risk jurisdictions post-FATF updates.	Flagged in monthly RFI report.
25	LQ2: Customer is being investigated for Terrorist Financing offences	Customer has been the subject of inquiry from any law enforcement agency relating to Proliferation Financing (PF) or/and terrorism or Terrorist Financing (TF) offences or terrorist related activities	Covered as part of AML screening.
26	LQ3: SEBI has passed order under SEBI Act, 1992 with Rules and Regulations made there under	Customer's name appears in any Order passed by IFSCA or SEBI. IFSCA or SFBI has initiated an investigation and has restrained individuals / entities from buying, selling or dealing in the securities markets, either directly or indirectly, in any matter.	Covered as part of AML screening.
27	LQ4: Struck off companies & LLPs and Disqualified Directors by ROC	Customer's name appears in the list of Struck-off Companies & LLPs and Disqualified Directors by Registrar of Companies or equivalent authority outside India. E.g. Such list is available on the website of the Ministry of Corporate Affairs (MCA).	Covered as part of AML screening.
28	MRI: Adverse media report about criminal activities of customer	Match of customer details with persons reported in media / open source for criminal offences	Covered as part of AML screening.
29	MR2: Adverse media report about Terrorist Financing offences or terrorist activities of customer	Match of customer details with persons reported in media / open source for Proliferation Financing (PF) or/and terrorism or Terrorist Financing (TF) offences or terrorist related activities	Covered as part of AML screening.
30	El l: Customer did not complete transaction	Customer did not complete transaction after queries such as source of fund etc.	FME actionable
31	El 2: 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.	FME actionable
32	El 3: Fraud/ attempted fraud to route transaction through impersonation	In case of fraud identities/ impersonation being used by the investors to route transactions. Any complaints received by any person about Fraud/ attempted fraud to route transaction through impersonation.	FME actionable
33	El 4: Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting.	FME actionable

SN	Alert Indicator	Indicative Rule/ Scenario- IFSCA	Ascent Remarks
34	El 5: Customer could not explain source of funds	Customer could not explain source of funds satisfactorily.	FME actionable
35	El 6: Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.	FME actionable
35	El 7: Transaction has no economic rationale	The amount or frequency or the stated reason of the transaction does not make sense for the particular customer.	FME actionable
36	El 8: Internal investigation by FMEs on a suspected case of front running / market abuse etc.	Internal investigation by FMEs on a suspected case of front running / market abuse / material breach of Code of conduct by employee(s) and their disclosed immediate relatives. Any internal assessment undertaken by FMEs/ appointed detective agencies/forensic audit/other such entities, revealing suspicion on asset liability mismatch of employees and/or checks ascertained from Depositories. Upon such identification, complete investment holdings of the identified PAN's across FMEs may be obtained from RTAs of Fund entities	FME actionable