# AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets

*(Updated as on 08.01.2026)*

## Table of Contents

**6. Record Keeping**

6.1 Obligations as per PMLA

6.2 Measures to be taken

**7. Other measures**

7.1 Approach to ICOs/ITOs

7.2 VDA transfers to/from unhosted wallet

7.3 Approach to unregistered VDA SPs

7.4 Approach on Anonymity enhancing crypto-tokens (AECs)

7.5 Approach on Tumbler/Mixer and other anonymity enhancing products/services

## Acronyms

| Term | Definition |
|---|---|
| AEC | Anonymity-Enhancing Crypto Tokens |
| AML | Anti-Money Laundering |
| CFT | Countering the Financing of Terrorism |
| CDD | Client Due Diligence |
| CPF | Combating Proliferation Financing |
| CRS | Common Reporting Standards |
| DNFBP | Designated Non-Financial Business and Profession |
| FATF | Financial Action Task Force |
| FI | Financial Institution (traditional financial institutions not defined as SPs) |
| FIU-IND | Financial Intelligence Unit - India |
| ICO / ITO | Initial Coin Offering / Initial Token Offering |
| Intermediary Service Provider | Refers to a Service Provider (SP) in a serial chain that receives and re-transmits a VDA transfer on behalf of the Originator SP and the Beneficiary SP or another intermediary SP |
| KYC | Know Your Customer |
| ML/TF/PF | Money Laundering, Terrorism Financing and Proliferation Financing |
| NFT | Non-Fungible Token |
| NRA | National Risk Assessment |
| OFAC | Office of Foreign Assets Control (US) |
| OTC | Over-the-Counter |
| P2P | Peer-to-Peer |

| | |
|---|---|
| PEPs | Politically Exposed Persons |
| PMLA | Prevention of Money Laundering Act 2002 |
| PMLR | Prevention of Money-laundering (Maintenance of Records) Rules 2005 |
| RBA | Risk-Based Approach |
| RE | Reporting Entities |
| SP | Service Provider providing services relating to Virtual Digital Assets |
| STR | Suspicious Transaction Reporting |
| UAPA | Unlawful Activities (Prevention) Act, 1967 |
| UNSC | United Nations Security Council |
| VDA | Virtual Digital Assets |
| VDA SP | Virtual Digital Asset Service Provider |

## 1. Introduction

### 1.1 Definition

Virtual Digital Assets have been defined in Section 2(47A) of the Income-tax Act, 1961 as:

a) any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means or otherwise, by whatever name called, [providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value], or [functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment scheme]; and can be transferred, stored or traded electronically;
b) a non-fungible token or any other token of similar nature, by whatever name called;
c) any other digital asset, as the Central Government may, by notification in the Official Gazette specify.

### 1.2 Legislative Framework

1.2.1 The *Prevention of Money-Laundering Act, 2002* constitutes the principal legislation forming the foundation of India's legal framework to combat money laundering. For the purposes of these Guidelines, "Money Laundering" shall have the meaning ascribed to it in Section 3 of the PMLA. The *Prevention of Money-Laundering Act, 2002* (hereinafter referred to as "PMLA") and Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (hereinafter referred to as "PMLR"), prescribes specific obligations, for Reporting Entities, relating to Client Due Diligence, Record-keeping, Transaction Monitoring and Reporting of prescribed transactions. Reporting Entities include 'Persons carrying on designated business or profession' which are defined under Section 2(1)(sa) of the PMLA. Sub-clause (vi) of the said clause includes, within its ambit, persons carrying on such other activities as may be designated by the Central Government, by notification, from time to time.

1.2.2 In order to address emerging money laundering and terrorist financing risks associated with Virtual Digital Assets (VDAs), the Government of India notified, vide Notification S.O. 1072(E) dated March 07, 2023, Virtual Digital Assets Service Providers (VDA SPs), engaged in the following activities, on behalf of another person in the course of business, as 'Reporting Entities':

i. Exchange between virtual digital assets and fiat currencies;
ii. Exchange between one or more forms of virtual digital assets;
iii. Transfer of virtual digital assets;

iv. Safekeeping or administration of virtual digital assets or instruments enabling control over virtual digital assets; and
v. Participation in and provision of financial services related to an issuer's offer or sale of a virtual digital asset.

The notification effectively brought VDA SPs within the AML/CFT/CPF regulatory framework, requiring them to comply with due diligence and reporting obligations similar to other reporting entities.

1.2.3 Subsequently, through Notification S.O. 4877(E) dated November 09, 2023, the *Director, Financial Intelligence Unit, India* was notified as the regulator of VDA SPs, appointed under Section 49(1) of the PMLA.

1.2.4 As per PMLR, the "Regulator" is defined under Rule 2(1)(fa), as a *person or an authority or a government which is vested with the power to license, authorise, register, regulate or supervise the activity of reporting entities or the Director as may be notified by the Government for a specific reporting entity or a class of reporting entities or for a specific purpose.*

1.2.5 Accordingly, FIU-IND has been designated as the AML/CFT/CPF regulator for Virtual Digital Asset Service Providers (hereinafter referred to as "Reporting Entities").

1.2.6 In this context, these Guidelines shall be known as the Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and Combating Proliferation Financing (CPF) Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets (hereinafter referred to as "the Guidelines"). The Guidelines provide a consolidated framework summarizing the provisions of the applicable laws and regulations governing AML, CFT, and CPF compliance in India, namely:

a) The *Prevention of Money-Laundering Act, 2002* (PMLA);
b) The *Unlawful Activities (Prevention) Act, 1967* (UAPA); and
c) The *Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005* (WMDA);

together with the rules framed thereunder and their applicability to VDA SPs.

1.2.7 These Guidelines prescribe the procedural and operational obligations to be followed by Reporting Entities (REs) to ensure compliance with AML/CFT/CPF measures, to identify and discourage any instances of money laundering, terrorist financing, or proliferation financing. This shall be carried out through implementing effective KYC, CDD, and ongoing due diligence measures; through transaction monitoring and suspicious transaction reporting; and record-keeping, to facilitate investigations by competent authorities.

### 1.3 Purpose of the Guidelines

The purpose of these Guidelines is to:

a) Promote understanding and application of Risk-Based Approach (RBA) and outline best practices for its effective implementation;
b) Incorporate Procedural safeguards to ensure fairness, transparency and legality.
c) Clear delineation of organizational responsibilities.
d) Guidance for operational readiness.
e) Establish an efficient reporting and compliance mechanism
f) Assist entities engaged in or seeking to engage in VDA activities to better understand and comply with AML/CFT/CPF obligations as prescribed under the PMLA and PMLR.

### 1.4 Scope and applicability

a) These Guidelines apply to all the Reporting Entities (REs) engaged in notified activities and detail the manner in which AML/CFT/CPF obligations are to be effectively implemented.
b) The Guidelines cover activities involving VDAs that are convertible to other funds or value, including both VDAs that are convertible to other VDAs and those convertible to fiat currency or that intersect with the fiat financial system.
c) Digital Rupee (e₹), Central Bank Digital Currency (CBDC) issued by the Reserve Bank of India (RBI) is excluded from the scope of these Guidelines as it represents a digital form of sovereign fiat currency.

It shall be noted that in accordance with the provisions of the PMLA, the obligations of VDA SPs are activity-based and apply irrespective of their physical presence in India. All entities irrespective of their registered location, if engaged in notified activities are required to register as Reporting Entity (RE) and comply with the prescribed AML/CFT/CPF obligations.

## 2. Registration of VDA SP with FIU- IND

### 2.1 Registration Requirement

a) In accordance with the provisions of the PMLA and the PMLR framed thereunder, registration with FIU-IND shall be a mandatory pre-requisite for VDA SPs engaged in any activity or operation as notified by the Central Government vide Notification S.O. 1072(E) dated March 07, 2023.

b) Non-registration shall be deemed a violation of the provisions of the PMLA and may invite action under Section 13(2) of the PMLA, in addition to any other enforcement measures as may be applicable.

c) Registration with FIU-IND is mandatory to ensure the maintenance of accurate and comprehensive records pertaining to each RE, including details of the Designated Director (DD), Principal Officer (PO), their principal place of business, significant business ownership etc.

### 2.2 Initiation of registration

a) The registration process will be initiated by the applicant VDA SP by registering the details of the reporting entity on the FINGate portal. Upon completion, the status will be displayed as '*awaiting approval*' and a temporary Reference ID will be generated, and an acknowledgement email will be sent to the applicant.

b) The Reference ID generated and provided to the applicant is only for reference and future correspondence with FIU-IND.

c) Formal registration shall be granted only after completion of due process including submission of prescribed documents, in-person meeting, and due approval by the Director, FIU-IND.

d) Upon satisfactory completion of the process, FIU Reporting Entity ID (FIU RE-ID) shall be generated and assigned to the applicant.

### 2.3 Submission of documents by the applicant

Applicant shall submit the following documents/information along with clearly stating whether entity is currently operational (if yes, since when) or yet to commence operations/under development (expected/tentative timeline). The scheduled in-person meeting shall be subject to operational readiness and submission of the following documents at least 15 days in advance.

### 2.4 Documents/Information Required to be submitted

a) Brief note on the nature of service and explanation on how the applicant's activities fall under the ambit of activities notified by Central Government (see para 1.2.2 above).
b) Corporate structure note including organogram and details of Significant Beneficial Ownership.
c) Copies of Incorporation Documents, Annual Returns, Balance Sheets, and Profit and Loss Accounts for the last three financial years as filed with MCA along with details of the registered office or principal place of business in India.
d) GST Returns for the last three financial years along with GST registration certificates in all operating states, clearly indicating the nature of activities.
e) Income Tax Returns and Form 26Q/26QF/26QE for TDS on VDA transactions.
f) Copies of all agreements or contracts (domestic or international) with exchanges, brokers, custodians, intermediaries, or other VDA SPs, along with a brief description of the scope and function of each arrangement.
g) PACT (Partner Accreditation for Compliance and Trust) certificate from VDA SPs registered with FIU-IND with whom the applicant has an ongoing or prospective business relationship (B2B, broker, or other).
h) A self-declaration to the effect that no proceeding has been initiated by, or is pending with any law enforcement authorities against the applicant or its directors/partners and no criminal cases are initiated, or pending against the applicant or its directors/partners.
i) A duly filled Questionnaire provided by FIU-IND, inter-alia pertaining to various aspects related to AML/CFT/CPF compliance.
j) A Cyber Security Audit Certificate issued by Indian Computer Emergency Response Team (CERT-In) empaneled auditor, affirming compliance with applicable cybersecurity frameworks and the CERT-In Directions dated April 28, 2022, issued under Section 70B(6) of the Information Technology Act, 2000. The audit shall be comprehensive and proportionate in coverage across all critical risk domains, and the audit report shall certify whether the audited environment is adequately safe to host and operate the notified VDA activities. The scope of the audit shall cover areas such as governance, compliance, access control and insider risk; infrastructure, network and endpoint security; application and AML systems security (including KYC, transaction monitoring, wallet security, cryptographic controls, backup and recovery); security of third-party, cloud services, exchange, custodian, and API risks; incident detection and response with CERT-In reporting readiness, etc.
k) Any other information or document, as required and intimated to the applicant, or any other additional details the applicant deems necessary to disclose for the completion of registration process.

The documents and information so submitted (in desired full and complete form) shall be subject to examination by FIU-IND. If found in order, an intimation for in-person meeting shall be sent to the applicant.

**2.5 In-person meeting**

2.5.1 In-person meeting is meant to ascertain and verify the AML/CFT/CPF compliance systems/processes/mechanisms/tools in place and shall be mandatorily attended by the Designated Director (DD) and the Principal Officer (PO).

2.5.2 During the in-person meeting, the applicant must provide a live demonstration/walkthrough of AML/CFT/CPF systems and tools, including KYC systems, Transaction Monitoring systems, Blockchain Analytics tools, Travel Rule compliance, Sanction Screening mechanisms and other applicable tools that enable the applicant to fulfil obligations under Chapter IV of the PMLA and PMLR, the laid down AML/CFT/CPF framework and these Guidelines.

2.5.3 The Director, FIU-IND reserves the right to deny or cancel registration if the applicant fails to fulfill its obligations under the PMLA.

## 3. GOVERNANCE FRAMEWORK

3.1 **Appointment of Designated Director** A "Designated Director (DD)" (as defined in Rule 2(1)(ba) of the PMLR) means a person designated by the reporting entity who shall be responsible for ensuring overall compliance with the obligations imposed under chapter IV of the PMLA and the PMLR.

3.1.1 The Designated Director shall ensure to evolve an internal mechanism for adherence to the procedures and manner of maintaining information in accordance with Rule 5 of the PMLR, including proper upkeep of CDD records, transaction records and documents required under the PMLA and PMLR.

3.1.2 The Designated Director shall ensure to evolve an internal mechanism for adherence to the procedure and manner of furnishing information to FIU-IND in accordance with Rule 7 of the PMLR.

3.1.3 The Designated Director shall ensure timely and accurate submission in respect of transactions prescribed under Rule 3 of the PMLR, any reports prescribed by FIU-IND and information sought by FIU-IND under Section 12A of the PMLA.

3.1.4 The Designated Director shall ensure to carry out risk assessment as prescribed under Rule 9(13) of the PMLR to identify, assess and take effective measures to mitigate ML/TF/PF risks.

3.1.5 The Designated Director shall oversee and ensure that officers and employees of the reporting entity follow all compliance procedures relating to record-keeping, CDD, transaction monitoring and reporting mandated under Chapter IV of the PMLA and the PMLR. It must be ensured that adequate resources, internal controls, processes and training are in place to support statutory AML/CFT/CPF compliance.

3.2 **Appointment of Principal Officer** A "Principal Officer (PO)" (as defined in rule 2(1)(f) of the PMLR), means an officer designated by the reporting entity provided that such officer shall be at the management level. The PO shall preferably be not below the level of Head Audit/Compliance/ Risk, and shall be responsible to ensure implementation and compliance with the obligations imposed under chapter IV of the PMLA and the PMLR. The REs (registered/prospective) are expected to ensure the following minimum requirements and qualifications with respect to the PO:

a) PO shall be exclusively engaged with a RE on a full-time basis and PO shall not undertake any simultaneous or concurrent engagement with any other entity in any capacity.

b) PO should have sufficient level of seniority and authority within the organization hierarchy to act independently without interference, bureaucratic constraints or improper influences.

c) PO should be familiar with AML/CFT/CPF legal requirements, reporting obligations, and enforcement mechanisms and shall have relevant experience (minimum three years) with appropriate skill set to fulfil obligations under PML Act, PML Rules and associated regulations.

d) The PO should have thorough knowledge of ML/TF risks and vulnerabilities relevant to his/her organization and the VDA and VDA SP sector. PO should also be aware of the emerging ML/TF trends and typologies.

e) PO should be a permanent invitee to the high-level committee(s) which evaluate risks associated with products and services to ensure that ML/TF risks posed by different products, services, transactions, clients, geographic areas etc. are appropriately identified, assessed, and mitigated.

f) With a view to enable the PO to effectively discharge his responsibilities, PO should have sufficient resources, including adequate support staff with necessary expertise, technical resources and unhindered and timely access to relevant information pertaining to client identification, Client Due Diligence information, transactions records and other relevant information, to ensure effective monitoring, reporting and implementation of the AML/CFT/CPF program

g) To respond promptly to requests for information made by FIU-IND and/or LEAs/regulators, PO may need to call information, documents etc. from relevant authorities within the organization. To enforce timelines and compliance in this regard, the REs should have appropriate internal guidelines for making available information to PO.

h) PO should place a review/status of AML/CFT/CPF function before the Board/Sub-committee of Board preferably on a quarterly basis.

i) PO should be based in India to ensure effective discharge of obligations under the PMLA framework.

j) To avoid conflict of interest, PO should be exclusively for responsibilities as cast under chapter IV of the PMLA and not be actively involved in business or operational activities of the RE.

k) The Principal Officer and the Designated Director should be separate individuals.

l) As per rule 7(1) of PMLR, the Name, Designation, address and contact details of the Designated Director and the Principal Officer shall be communicated promptly to FIU-IND. The same shall be updated through the FINGate portal.

### 3.3 Roles and Responsibilities of the Principal Officer

a) The Principal Officer (PO) shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the PMLA and the PMLR.

b) As prescribed under Rule 7(2), the PO shall furnish the information referred to in Rule 3(1) of the PMLR to FIU-IND on the basis of information available with the reporting entity. A copy of such information shall be retained for the purposes of official record.

c) As prescribed under Rule 8(2), the PO shall, on being satisfied that the transaction is suspicious, furnish the information promptly to FIU-IND.

d) The PO shall evolve and implement an internal mechanism, with regard to any directions/ guidelines issued by FIU-IND, for furnishing information as prescribed under Rule 3(1) of the PMLR. With regard to the escalation of prospective suspicious transactions, special attention shall be paid to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should be examined and the findings at PO level should be properly recorded. Such records and related documents should made available to relevant authorities, as required, to scrutinize such transactions. These records are required to be preserved for five years as is required under PMLA.

e) While the activities of analyzing alert and preparing the documents for managing the alert can be delegated within the AML compliance team, the ultimate analysis and decision-making rests with the PO. The records verified by and papers related to this decision need to be recorded and retained for audits.

f) The PO shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction is escalated to PO.

g) Where the PO is of the opinion that a transaction is not reportable, decision on closure of alert shall be taken by the PO and it must be ensured that reasons for not reporting such transactions are clearly recorded.

h) The PO shall review the list of alerts and the approach from time to time to ensure that the reporting mechanism is complete and is in line with the expectations. It is equally important that the PO conducts surprise checks of the data being monitored by the AML compliance unit and check transaction on sample basis, to ensure that there is no gap and all unusual/potential suspicious transactions have been highlighted to the PO on ongoing basis.

i) The PO and the staff assisting him in execution of AML/CFT guidelines shall have timely access to information including customer identification data, other KYC information and records.

j) The PO appointed for AML/CFT/CPF compliance shall report directly to the Board or a designated Committee of Board of the RE. Furthermore, the PO shall, on a periodic basis and/or basis the frequency determined by the Board, but not later than one year, report at the minimum the following items:

   i. Assessment of the effectiveness of RE's AML/CFT/CPF compliance program.
   ii. Any identified risks or vulnerabilities in the program.
   iii. Summary of Suspicious Transaction reports (STRs), other reports prescribed in PMLA/PMLR and any other information/reports prescribed by FIU-IND, submitted to FIU-IND.
   iv. Any Instructions, Red flag indicators, Typologies, Guidance etc. issued by FIU-IND from time to time, and their implementation status.
   v. Any proposed changes to the AML/CFT/CPF policy of the RE.

**3.4 AML/CFT/CPF Policies and procedures**

3.4.1 In accordance with the Rule 9(14)(ii) and (iii), every RE needs to formulate and implement AML/CFT/CPF Policies and procedures (hereinafter referred to as "Policies") in order to combat the menace of money-laundering, terror financing, proliferation financing and other related serious crimes. Rule 7(3) of the PMLR casts an obligation on every reporting entity to evolve an internal mechanism to detect transactions as specified under Rule 3 and furnishing information about such transactions to FIU-IND.

3.4.2 It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of furnishing information under Rule 5 and Rule 7 of the PMLR.

3.4.3 To comply with the statutory obligations under Chapter IV of the PMLA, every RE shall establish appropriate Policies for the prevention of ML, TF, and PF, and ensure their effectiveness in compliance with all relevant legal and regulatory requirements. The REs shall:

a) Issue a statement of Policies, on a Group basis where applicable, for dealing with ML, TF and PF risks, as per rule 3A of the PMLR, reflecting the current statutory and regulatory requirements. The term "Group" shall have the same meaning assigned to it in Rule 2(1)(cba) of the PMLR.
b) Ensure that the spirit of these Guidelines and Policies are communicated and understood by the Management, all officers and staff members;

c) Conduct an independent annual review of the Policies to assess their continued effectiveness. Such review shall be undertaken by person(s) other than those involved in framing the Policies.
d) Adopt client acceptance policies and procedures and undertake Client Due Diligence (CDD) measures to the extent that is sensitive to the risk of ML, TF and PF depending on the type of client, business relationship, transaction behavior, geographic areas, products, services etc.;
e) Have a system in place for identifying, monitoring and timely reporting of suspicious transactions, threshold-based reports, typologies with ML/TF/PF risk etc. to FIU-IND.
f) Have internal mechanism in place for furnishing any records/information to FIU-IND within such time and in such manner as desired by FIU-IND under Section 12A of the PMLA;
g) Have mechanism for cooperation with law enforcement agencies, including timely disclosure of required information.
h) Ensure that product/services of any third party based in known high risk jurisdictions are not utilized/availed.

3.4.5 Every Reporting Entity shall ensure that a clear, comprehensive, and concise summary of its Policies is prominently displayed and made accessible on its official website and/or mobile application accessed by the users for onboarding and login.

**3.5 Client Acceptance framework**

In order to identify the types of clients that are likely to pose a higher ML/TF/PF risk, the RE shall have Board approved client acceptance framework. The framework shall include the following:

a) No relationship or transaction shall be initiated without implementing the appropriate CDD measures.
b) RE shall not allow the opening of or keep any anonymous account or account in fictitious names or accounts on behalf of other persons whose identity has not been disclosed or cannot be verified.
c) It shall be ensured that any discrepancy, mismatch, or non-verification of information shall result in triggering of enhanced measures, as applicable.
d) In cases where the RE is not able to ascertain the identity of the client, or the information provided by the client is suspected to be false or non-genuine or appropriate CDD measures, or enhanced measures under CDD cannot be applied, it shall result in termination of the onboarding process and no transaction shall be allowed for such client.
e) System shall be implemented to ensure that the identity of the client does not match with any person or entity appearing in the Sanctions lists.

f) In case RE does not have records of the identity of its existing clients, as prescribed under para 4 of these Guidelines, it shall obtain the records in a time-bound manner, failing which the reporting entity shall close the account of the clients after giving due notice to the client.

### 3.6 Internal control and Oversight

#### 3.6.1 Risk Assessment

a) REs shall carry out Risk Assessment exercise periodically to identify, assess and take effective measures to mitigate its ML/TF/PF risk, severally and together, for clients, geographic areas, products, services, transactions etc.
b) Risk assessments must be designed and implemented to assist REs to better understand their risk exposure and areas in which they should prioritize allocation of resources for appropriate control and oversight of their AML/CFT/CPF activities.
c) A key component of the Risk assessment may entail that REs shall identify areas where their products/services could be exposed to ML/TF/PF risks e.g. VDAs, VDA related products or services (in particular, methods in which Anonymity Enhanced Transactions can be conducted); VDA related business and professional practices; and technologies/tools associated with VDA Activities; client carrying out extremely complex or high value transactions; client carrying out transactions with known high-risk jurisdictions etc. Further, prior to the launch of new technologies, products, services etc., REs shall carry out proper risk assessment to identify, assess and mitigate the ML/TF/PF risks that may so arise.
d) The risk assessment by the RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board in alignment with the outcome of the previous risk assessment exercise. However, it must be ensured that the assessment is carried regularly, and the interval between any two assessments shall not exceed one year.
e) The outcome of the risk assessment exercise and mitigation measures identified/ implemented shall be put up to the Board, and should be made available to the relevant authorities as and when required.

#### 3.6.2 Risk Classification of Clients

RE shall have Board approved framework broadly laying down principles for risk classification of its clients. The framework shall include the following:

a) The clients shall be classified at the minimum under two categories, viz. High risk and Medium risk. REs may develop further categories over and above these categories for clients with higher risk perception. The parameters and factors for determining risk perception under each category including those relevant for suspicious transaction monitoring and application of enhanced measures under CDD shall be clearly defined and objectively laid out.
b) Risk classification of the clients shall be undertaken based on parameters such as client's identity, financial position, nature of business activity, information about the client's business and their location, geographical risk covering clients as well as transactions, type of products/services offered, types of transaction undertaken etc.
c) A system of periodic review of risk classification of the accounts, with such periodicity being at least once in six months shall be put in place.
d) The risk classification of a client and the specific reasons for such classification shall be kept confidential.

### 3.6.3 Independent Review of Policies and procedures

The REs shall cause an independent annual audit of its AML/CFT/CPF controls, systems, procedures and safeguards and shall undertake corrective actions for deficiencies, if any. The internal audit shall be conducted at least once a year, and focus particularly on compliance with Policies, procedures and controls relating to AML/CFT/CPF. The audit reports should specifically comment on the robustness of the Policies and internal processes and make suggestions where necessary, to strengthen the Policy and implementation. The report shall be placed to the Board or a designated Board Committee of the RE.

### 3.7 Capacity building

a) REs shall ensure that adequate screening mechanism is put in place as an integral part of their recruitment process of personnel.
b) REs shall have an ongoing employee training programme to ensure that members of staff are adequately trained in implementing AML/CFT/CPF measures.
c) Instruction manuals on the procedures for client on boarding, CDD, Sanctions screening, record-keeping, transaction monitoring etc., as per the Policy shall be set out.
d) REs shall ensure that training requirements and program are specifically customized for the staff handling issues arising from AML/CFT/CPF.

## 4. CLIENT DUE DILIGENCE MEASURES

### 4.1 Client due diligence

4.1.1 Keeping in view the anonymous and instantaneous nature of VDA transactions and the potential of services offered by REs being misused by illicit actors for the purpose of money laundering, terror financing and proliferation financing, all REs must have a robust Client due diligence (CDD) mechanism in place.

4.1.2 The CDD shall be used to verify the identity of a client, including when establishing relationship with the client; when RE does not have records of identity of its existing clients; when there is suspicion of ML/TF/PF, regardless of any thresholds; when there is doubt about the veracity or adequacy of previously obtained identification information/ documents; and for carrying out periodic profile updation of the existing clients.

4.1.3 In accordance with rule 9 of the PMLR, every RE shall identify and verify the identity of its clients at the time of establishing relationship and thereafter at periodic intervals or upon any doubt about the authenticity or adequacy of previously obtained information.

4.1.4 The Client Due Diligence (CDD) process shall, *inter alia*, include but not limited to:

a) Identifying clients by obtaining their details/documents; verifying their identity using reliable and independent sources of identification; developing a client risk profile based on holistic assessment of available and open-source information; Ongoing due diligence through continuous monitoring of client transactions and activities; and updating client information periodically or when triggered by changes in their profile.
b) Collect additional identifiers such as IP address with timestamp, Geo-location, Device ID, VDA wallet addresses, Transaction hashes among other parameters, which are considered necessary for verification, authentication, monitoring, and risk assessment purposes.
c) Mandatorily obtaining and verifying the Permanent Account Number (PAN) of client for onboarding, and/or undertaking any VDA related activity. The REs shall ensure compliance with this requirement as part of their CDD measures.

### 4.2 CDD Measures for Individual

4.2.1 REs shall obtain the following minimum client information to be captured at time of establishing relationship.

(a) **Personal Information:**

i. Full name as appearing in the PAN;
ii. Date of birth;
iii. Gender;
iv. PAN details
v. Identity document type
vi. Identity document no.
vii. Nationality

(b) **Contact Details:**

i. Address;
ii. Mobile number;
iii. Email ID

(c) **Financial and Occupation Details:**

i. Occupation;
ii. Income range;
iii. Bank account details

(d) **Other Parameters:**

i. Selfie of the client with liveness detection;
ii. Latitude and longitude coordinates of the onboarding location with date and timestamp alongwith IP address

4.2.2 For the purpose of CDD of its clients, RE is required to collect PAN and any one of the following identity documents: - Passport, Driving License, Proof of possession of Aadhaar number, Voter's Identity Card issued by Election Commission of India; or the equivalent e-document thereof containing the details of identity and address.

4.2.3 The RE shall verify and validate the client information and documents furnished for CDD purpose through reliable and independent sources of identification. The Mobile Number and Email ID verification shall be carried out through One-Time Password (OTP) validation and/or link verification.

4.2.4 The RE shall ensure that the client whose credentials is being furnished is the same individual who is actually accessing the application and personally initiating the account creation process. The authenticity of such access and personal presence shall be established by capturing a live photograph of the client and employing liveness detection technology to verify the client's physical presence at the time of onboarding.

4.2.5 The onboarding system shall be equipped to accurately capture the geo-location coordinates (latitude and longitude) of the client in order to establish the precise location at which the verification process is undertaken. In case of mismatch between the address furnished and geo-coordinates, enhanced measures under CDD must be undertaken.

4.2.6 Verification of the client's bank account shall be carried out through a penny-drop mechanism, for the purpose of confirming both ownership and operational status of the account.

**4.3 CDD Measures for legal person who is not a natural person**

4.3.1 For opening an account of legal person who is not a natural person (sole proprietary concerns, partnership firms, companies, trusts, Non-profit organization etc.), Client Due Diligence (CDD) of the legal person shall be carried out in accordance with the procedure as prescribed above for individuals under these Guidelines, where in it shall be mandatory to obtain and verify PAN from issuing authority database in all cases. In addition, REs shall also obtain the information and applicable documents prescribed in Rule 9 of the PMLR.

4.3.2 The RE shall ensure that the beneficial owner(s) is/are determined for all clients and all reasonable steps in terms of Rule 9(3) of the PMLR shall be undertaken to verify his/her identity.

4.3.3 In case of clients who are non-profit organization (as defined in 2(1)(cf) of the PMLR). REs shall ensure that such clients are registered on the DARPAN Portal of NITI Aayog, as prescribed under Rule 9(9A) of the PMLR.

**4.4 Enhanced measures under CDD**

4.4.1 RE shall apply enhanced measured under Client Due Diligence (CDD) based on materiality and risk. The measures shall be initiated for transactions assessed as high risk or where ML/TF/PF concerns arise based on any of the red flag indicators triggered. Conducting enhanced measures under CDD mean applying measures and procedures that are more rigorous and robust than standard CDD and KYC processes. The scope and intensity of these measures shall be commensurate with the risk profile of the client and circumstances which triggered such measures, and should not be limited to merely obtaining income/turnover related documents. The following are indicative and non-exhaustive reasonable measures to be considered while implementing enhanced measures under CDD:

a) Take measures to examine the financial position, including source of funds of the client;
b) Take measures to record the purpose behind conducting such transactions;
c) Conduct more frequent review of the client's profile/transactions;

d) Take reasonable measures like gathering information from open sources;
e) Undertaking independent verification of the information obtained from the client and consulting independent and credible databases, where necessary.

4.4.2 REs shall mandatorily apply enhance measures under CDD to relationships and transactions in the following cases:

a) with natural and legal persons from known high-risk jurisdictions, specifically with countries designated as tax havens and those on the FATF grey and black lists;
b) when establishing relationship with Politically Exposed Persons ("PEPs"). For the purposes of these guidelines, 'PEP' shall have the same meaning assigned to it as per Rule 2(1)(db) of the PMLR;
c) clients who are Non-profit organization.

In cases where the RE is not able to undertake the required enhanced measures under CDD, the RE shall terminate the relationship and file a Suspicious Transaction Report (STR) with FIU-IND, in accordance with rule 10(3) of PMLR.

**4.5 Periodic CDD updation**

4.5.1 Given the high-risk nature of Virtual Digital Assets (VDAs), periodic updation of CDD on existing clients shall be undertaken. Such periodic review shall form part of the RE's risk-based approach (RBA) framework and shall include necessary verification or enhanced measure under CDD where material changes in ownership, business, or transaction behavior are observed.

4.5.2 Under the risk-based approach REs shall ensure that all Client Due Diligence (CDD) information and data remains accurate, up to date and relevant. For client assessed as high risk, KYC updation shall be carried out at least once every six months. For all other clients, KYC updation shall be carried out at least once every year, measured from the date of account opening or the last KYC updation.

4.5.3 The policy governing periodic KYC updation shall be clearly documented within the RE's CDD program, duly approved by the Board. Client's for whom periodic updation of KYC has already fallen due, the REs shall ensure that accounts of such clients are subject to KYC updation on priority.

a) **No change in CDD information:** In case of no change in the CDD information of the client, a self-declaration in this regard shall be obtained from the client. Further, REs shall ensure during this process that ultimate Beneficial Ownership (BO) information available with

them in case of legal person is accurate and shall ensure that it is kept up to date. A self-declaration in this regard shall be obtained from the client.

b) **Any change in CDD information:** In case of change in any CDD information, RE shall undertake the CDD process equivalent to that applicable for on-boarding a new client including verification.

c) REs shall ensure that the validity of the CDD documents available with the RE has not expired. In such cases, the RE shall undertake the CDD process equivalent to that applicable for on-boarding a new client.

d) It shall be ensured that the information/documents obtained from the clients at the time of updation/ periodic updation of KYC are promptly updated in the records / database of the REs and a record mentioning the date of updation of CDD details, is also maintained.

e) Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the REs such as requirement of obtaining live Selfie/Video, requirement of physical presence of the client, a more frequent periodicity of KYC updation shall be clearly specified in the RE's CDD program.

4.5.4 REs shall advise the clients that in order to comply with the PMLR, in case of any update in the information/documents submitted by the client at the time of establishing relationship, clients shall promptly intimate and submit to the REs the update of such information/documents.

## 5. ONGOING DUE DILIGENCE AND TRANSACTION MONITORING

### 5.1 Ongoing Due Diligence

In accordance with rule 9 (12) of the PMLR, the RE shall exercise Ongoing due diligence (ODD) by closely examining and scrutinizing transactions on a continuous basis, to determine whether client transactions are consistent with the REs knowledge of the client, its financial/risk profile, and the source of funds. The extent and intensity of monitoring shall be aligned with the risk category of the client. ODD also involves identifying changes in the client's risk profile (e.g., the client's behavior, type of VDA products/services availed, and the volume and value involved in such transaction) and keeping it up to date, which may necessitate the application of enhanced measures under CDD.

### 5.2 Transaction Monitoring

5.2.1 REs shall establish an internal mechanism to monitor the transactions through their systems on continuous basis, and as per the Guidances issued by FIU-IND for detecting suspicious transactions from time to time. To implement this, REs shall develop, implement, and maintain effective transaction monitoring systems (including intermediary REs and cases where the originator and/or beneficiary wallet is hosted by them) that can identify the origin and destination of a VDA, and apply robust controls to detect potential ML/TF/PF activities.

5.2.2 REs should be able to flag any unusual or suspicious movement of funds or activity that may indicate potential illicit behavior or activity, including fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat transactions. Transaction monitoring program should be appropriate to the scale and size of the RE and the products/services it provides. In the transaction monitoring process, the RE shall put in place appropriate systems to incorporate red flag indicators, guidance, typologies, instructions etc. issued by FIU-IND from time to time, along with any additional indicators identified through its own risk assessment. All alerts generated shall be reviewed by the AML/CFT/CPF monitoring team and PO without delay, and wherever applicable, STRs shall be filed promptly with FIU-IND.

5.2.3 REs shall deploy appropriate, scalable and secure systems to enable to store transaction data so as to enable reconstruction of individual transactions in compliance with Rule 4 of PMLR. These systems shall integrate seamlessly with existing systems, provide role-based access control, with reliable data backup and recovery mechanisms.

5.2.4 As large volumes of transactions are carried out on a continuous basis, REs may employ transaction risk scoring models, and deploy automated systems. REs may consider adopting

appropriate innovations including artificial intelligence and machine learning (AI/ML) technologies to support effective monitoring.

**5.3 Travel rule**

5.3.1 In accordance with Rule 4 of the PMLR, it is required that all necessary information be maintained by the RE to permit reconstruction of individual transactions. This would be applicable to VDA transfers from a client holding a wallet with a RE or using its services to transfer VDAs to a wallet hosted by another RE. In this case, the originating RE shall undertake CDD measures and sanction screening on the counterparty before they transmit the required information to avoid dealing with illicit actors or sanctioned person/entity unknowingly.

5.3.2 In terms of Rule 4 of the PMLR, REs shall ensure to include required and accurate originator information, and required beneficiary information, on VDA transfers and related messages. REs shall also monitor transfers to detect those which lack the required originator and/or beneficiary information.

5.3.3 REs facilitating or involved in VDA transfers, either as an originating or beneficiary entity, shall deploy appropriate technological solution that shall enable the originating and beneficiary RE to comply with its AML/CFT/CPF obligations for obtaining, holding, and transmitting the required information to maintain transparency of Virtual Digital Asset (VDA) transactions. In exceptional cases where deployment is found not feasible self-declaration based mechanism may be used.

This shall enable the REs to carry out the following actions:

a) enable the submission of required and accurate originator and required beneficiary information immediately (means that providers should submit the required information prior, simultaneously or concurrently with the transfer itself) and securely (means that providers should transmit and store the required information in a secure manner to protect the integrity and availability of the required information and facilitate record keeping) when a VDA transfer is conducted. The information shall be made available on request to appropriate authorities without any delay.
b) provide with a communication channel to support further follow-up with a counterparty RE for the purpose of counterparty due diligence; and requesting information on a certain transaction to determine if the transaction involves high risk or prohibited activities or sanctioned person/entities etc.

5.3.4 It shall be noted that post-facto submission of the required information is not permitted (i.e., submission must occur before or when the VDA transfer is conducted).

5.3.5 The required information, which the originating RE must obtain, hold and transmit, includes

a) Originator's Permanent Account Number (PAN) and Originator's identity document No.
b) Originator's name (i.e., the sending person's verified full name).
c) Originator's wallet address/account number used to process the transaction
d) Originator's physical (geographical) address that uniquely identifies the originator to the originating RE, and date of birth, provided that such an address has been verified for accuracy by the originator RE as part of its CDD process
e) Beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VDA transfer). This is not required to be verified by the originating RE for accuracy, but should be reviewed for the purpose of sanction screening, transaction monitoring and STR filing
f) Beneficiary wallet address/account number used to process the transaction

5.3.6 The required information which the beneficiary RE must obtain from the originator RE and hold, includes: which includes:

a) Originator's Permanent Account Number (PAN) and Originator's identity document No.
b) Originator's name (i.e., the sending person's name). The beneficiary institution does not need to verify the originator's name for accuracy, but should review it for the purpose of sanction screening, transaction monitoring and STR filing
c) Originator's wallet address/account number used to process the transaction.
d) Originator's physical (geographical) address that uniquely identifies the originator to the originating RE, and date of birth
e) Beneficiary's name (i.e., the name of the person who is identified by the originator as the receiver of the VDA transfer). The beneficiary RE must verify the beneficiary's name for accuracy. Thus, the beneficiary RE shall be able to confirm if the beneficiary's name and account number they obtain from the originating RE match with the beneficiary RE's verified client data
f) Beneficiary's wallet address/account number used to process the transaction

5.3.7 Summary of the data requirement for originating and beneficiary REs for compliance with the travel rule is presented below in **Table1**:

**Table-1**

| **Data item and required action** | **Originating RE** | **Beneficiary RE** |
|---|---|---|
| Originator information | Required i.e., submitting the necessary data to a beneficiary RE is mandatory. | Required, i.e. the beneficiary RE needs to obtain the necessary data from originating RE. |

| | | |
|---|---|---|
| | the originating RE needs to verify the accuracy as part of its CDD process. | The beneficiary RE may assume that the data has been verified by the originating RE. |
| Beneficiary information | Required, i.e. submitting the necessary data to the beneficiary RE is mandatory.<br>The originating RE must monitor to confirm no suspicions arise. | Required, i.e. the beneficiary RE needs to obtain the necessary data from the originating RE.<br><br>the beneficiary RE must have verified the necessary data and needs to confirm if the received data is consistent. |
| Action required | Obtain the necessary information from the originator client and retain a record.<br><br>Screen to confirm that the beneficiary is not a sanctioned name.<br><br>Monitor transaction and report when it raises a suspicion. | Obtain the necessary information from the originating RE and retain a record.<br><br>Screen to confirm that the originator is not a sanctioned name.<br><br>Monitor transaction and report when it raises a suspicion. |

**5.4 Sanctions Screening**

5.4.1 Sanctions screening shall be carried out minimum in each of the following times at the (i) time of onboarding, (ii) during change in KYC details, (iii) change in sanction lists. Furthermore, sanction screening should also be done at the time any VDA transaction is initiated.

5.4.2 REs must ensure prompt application of the directives when issued by the competent authorities for implementing United Nations Security Council Resolutions (UNSCRs) relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions.

5.4.3 REs must also ensure prompt application of the directives when issued by the competent authorities relating to the individuals designated as 'terrorist' under the Unlawful Activities (Prevention) Act, 1967 (UAPA) and directives when issued by the competent authorities under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMDA).

5.4.4 REs shall put in place appropriate safeguards to ensure that no VDA transfers are completed without sanction screening, which may include putting a wallet on hold until screening is completed and confirmed that no concern is raised; and/or arranging to receive a VDA transfer with a provider's wallet that links to a client's wallet and moving the transferred VDA to their client's wallet only after the screening is completed and has confirmed that no concern is raised.

**5.5 Suspicious Transaction Report (STR)**

5.5.1 In accordance with Rule 7(2) and Rule 8(2) read with Rule 3(1)(D) of the PMLR, REs shall promptly furnish information in respect of suspicious transactions identified through transaction monitoring, including attempted suspicious transactions, to FIU-IND.

5.5.2 An alert serves as the initial step in detecting a suspicious transaction and acts as a red flag triggered by a potentially suspicious activity. The RE shall put in place robust systems and processes to generate alerts based on predefined red flag indicators (RFIs). The principles for implementing RFIs, along with common minimum alerts and parameters for generating these alerts should be in line with the Guidances issued by FIU-IND for detecting STRs from time to time, under Rule 7(3) of PMLR,.

5.5.3 The format for reporting transactions, including suspicious transactions made or attempted, as required under Rule 7(3) and Rule 8(2) of the PMLR, shall be as prescribed by FIU–IND from time to time. Reports submitted with FIU-IND should contain complete and accurate information in respect of client KYC, Wallets, Transactions, Counterparties, Grounds of Suspicion etc.

5.5.4 Identification and reporting of STRs is an extremely serious obligation cast on the REs under the PMLA. RE is expected to ensure that every STR is reported to FIU-IND only after due application of mind and after necessary diligence. A prerequisite for high-quality STR reporting is ensuring that every data point available with an RE is effectively leveraged. This would include KYC information, transactional information, technical/metadata information, IP Addresses, Device IDs and any behavioral insights. RE are expected to make serious efforts towards reporting high quality STR which serves as a critical tool in detecting, deterring, and investigating the flow of illicit funds.

5.5.5 REs shall file an STR, irrespective of the amount of transaction and/or the threshold limit envisaged for reporting under PMLA, if they have reasonable grounds to believe that the transactions involve proceeds of crime or financing of terrorism.

### 5.6 Prohibition on Tipping-off

Section 12(2) and Section 12A(3) of the PMLA read with Rule 8(6) of the PMLR require REs, their directors, officers, and all employees (permanent as well as contractual) to ensure that the fact of maintenance of records and furnishing of information to FIU-IND is kept confidential. This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, REs shall ensure that there is no tipping off to the client or any other person at any level.

### 5.7 Submission of other reports to FIU-IND

REs shall furnish a Monthly Report in such form, time and manner as may be prescribed by FIU-IND from time to time. The Report shall include essential metrics, activity indicators, compliance status and other relevant details as deemed necessary, in a consolidated manner as prescribed by FIU-IND from time to time.

## 6. Record Keeping

### 6.1 Obligations as per PMLA

REs shall retain records as specified under Sections 12(1)(a) and 12(1)(e) of the PMLA. The Reporting Entity shall ensure that such documents and records are securely preserved and not destroyed during the retention period.

### 6.2 Measure to be taken

The following steps shall be taken regarding maintenance, preservation and reporting of client information. The REs shall,

a) Maintain and preserve the records pertaining to the client identification and their addresses obtained while onboarding and during the course of business relationship, for at least five years after the account-based relationship is ended;

b) Maintain and preserve all necessary records of transactions for at least five years from the date of transaction;

c) Where the records relate to ongoing investigations or transactions that have been the subject of a disclosure, such records shall be retained until it is confirmed that the case has been closed. Wherever practicable, the RE shall seek and retain relevant identification documents for all such transactions and report any suspicious transactions;

d) Maintain all necessary information and records in respect of transactions so as to permit reconstruction of individual transaction, including the following:

   i. the nature of the transactions;
   ii. the amount and types of VDA and/or the fiat currency involved, if any, in the transaction;
   iii. the date on which the transaction was conducted;
   iv. the parties to the transaction;
   v. Any other details as specified for compliance of travel rule.

e) Implement a system with clearly defined procedures for the retention, maintenance, and preservation of all transaction and account records as required under the PMLA, PMLR Rules, and these Guidelines. The system shall enable records and data to be retrieved easily and promptly whenever required or requested by competent authorities;

f) Preserve complete audit trails, including verification responses, timestamps, and authentication logs, in a tamper-proof manner;

## 7. Other measures

### 7.1 Approach to ICOs / ITOs

7.1.1 Initial Coin Offerings (ICOs)/ Initial Token Offerings (ITOs) are generally a means to raise funds for new projects from early backers and function similar to IPOs for stock offerings. However, such activities present heightened and complex ML/TF/PF risks, as they lack justified economic rationale, established and comprehensive mitigation measures, and full and transparent disclosures. Persons offering services relating to issuance, offer, book building, underwriting, market making and placement agent activity, sale, distribution, ongoing market circulation and trading of a VDA would be considered as REs under these guidelines.

7.1.2 The use of an automated process such as a smart contract to carry out RE functions does not relieve the parties of responsibility and obligations under Chapter IV of the PMLA and PMLR. In such instances, controlling parties (responsible for the execution of the contracts) qualified as REs shall be required to undertake documented ML/TF/PF risk assessments prior to the launch or use of the platform and put in place robust and demonstrable risk mitigation control.

7.1.3 Given the inherently elevated risks and the potential for misuse, ICO/ITO-related activities are strongly discouraged.

### 7.2 VDA transfers to/from unhosted wallet

7.2.1 In cases where the VDA transfer and transaction is between two wallets where at least one of them is a hosted wallet, the onus of compliance would be on the RE where the wallet is hosted. REs undertaking such transaction should evolve an internal mechanism to obtain the required originator, beneficiary and other relevant information from their client. Such transfers shall fall within scope of the REs broader AML/CFT/CPF obligations.

7.2.2 VDA transfers and transaction to/from unhosted wallets and related P2P transaction poses significant risks due to anonymity, the lack of limits on portability, mobility, transaction speed, and usability. Therefore, REs shall collect data on unhosted wallet transfers, and monitor and assess that information as necessary to determine the risk posed by such transaction, and then apply appropriate enhanced measures under CDD and other risk-based controls to such transaction and client, as detailed in the Guidelines.

7.2.3 REs may choose to impose additional limitations, controls, or prohibitions on transactions with unhosted wallets in line with their risk assessment. Potential measures include enhancing

existing risk-based control framework to account for specific risks posed by transactions with unhosted wallets (e.g., accounting for specific users, patterns of observed conduct, geographical risks, information from LEA and other relevant agencies) and/or enabling only those transactions assessed to be reliable.

### 7.3 Approach on unregistered VDA SPs

Similar reasoning, as detailed in *para 7.2* above, shall apply in considering the risks posed by REs that are not yet registered with FIU-IND. It is reiterated that the obligations of VDA SPs are activity-based and apply irrespective of their physical presence in India. All entities irrespective of their registered location, if engaged in notified activities, are required to register with FIU-IND as Reporting Entities (REs). A VDA SP not registered with FIU-IND shall be liable for compliance action initiated under Section 13 of the PMLA.

### 7.4 Approach on Anonymity enhancing crypto-tokens (AECs)

In line with the risk-based approach and based on the risk assessment under Rule 9(13)(i) of the PMLR, such transactions are deemed to be unacceptably high risk and as such outside the acceptable risk appetite due to their inherently elevated ML/TF risks. REs shall refrain from permitting deposits or withdrawals of Anonymity-Enhancing Crypto Tokens (AECs) or VDAs designed to conceal or obfuscate the origin, ownership, or value of transactions. Accordingly, Reporting Entities shall consider dealings in AECs as not permissible within their risk-mitigation framework and such transactions shall not be facilitated.

### 7.5 Approach on Tumbler/Mixer and other anonymity enhancing products/services

Similar reasoning, as detailed in *para 7.4* above, shall apply in transactions involving crypto tumblers, mixers, and other anonymity-enhancing products or services. REs shall deploy appropriate transaction monitoring and analytical tools to identify such transactions and upon detection, these transactions shall not be facilitated and must trigger suitable risk mitigation measures.

**********