SATYA MICROCAPITAL LIMITED

Know Your Customer (KYC) and
Anti- Money Laundering (AML) Policy

V.2.4

November 2025

1. Objective

The Know Your Customer and Anti-Money Laundering (the Policy) applies to SATYA MicroCapital Limited (hereinafter referred to as 'SATYA' or 'the Company'). This Policy requires the Company and each employee to:

- Protect the Company from being used for money laundering or funding terrorist activities.
- Conduct themselves in accordance with the highest ethical standards.
- Comply with the letter and the spirit of applicable Anti-Money Laundering (AML) Laws, and the Company's KYC & AML procedures.
- Be alert to and escalate suspicious activity and not knowingly provide advice or other assistance to individuals who attempt to violate or avoid money-laundering laws, or this Policy; and
- Co-operate with the regulatory authorities and the Financial Intelligence Unit as per the applicable laws.

2. Applicability & Validity of the Policy

The Policy shall be applicable from such date as approved by the Board of Directors. The Board shall review, validate, update, and approve the Policy as applicable from time to time. Any revisions in specific aspects of this Policy may be communicated through mandates issued by the relevant authority and shall become part of this Policy from the date they become effective.

3. Regulatory Reference

RBI vide its circular no. RBI/2015-16/108 DNBR (PD) CC No. 051/03.10.119/2015-16 as duly amended from time to time has instructed all the Non- Banking Finance Company (NBFCs) to adopt the necessary guidelines depending on the activity undertaken by them and ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of the Board. Therefore, this Policy is thus being designed in line with Master Direction - Know Your Customer (KYC) Direction, 2016, issued by the RBI, as amended from time to time ("KYC Master Directions")Prevention of Money Laundering Act -2002, Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and such other regulatory laws as may be applicable.

4. Definitions

For the purpose of KYC Norms, definition of various terms used is as under:

1.1 "**Aadhaar number**" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

1.2 "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

1.3 **"Authentication"** in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other

Subsidies, Benefits and Services) Act, 2016.

1.4 **Beneficial Owner (BO)**

(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 person, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

i) "Controlling ownership interest" means ownership of/entitlement to more than 10 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 10 per cent of capital or profits of the partnership or who exercises control (including right to control the management or policy decision) through other means.

(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/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (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 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

1.5 **Central KYC Records Registry (CKYCR)** means an entity defined under Rule 2(1) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KY records in digital form of a customer.

1.6 **"Certified Copy"** - Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid documents produced by the customer with the original and recording the same on the copy by the authorized officer of the RE as per the provisions contained in the Act.

1.7 **"Counterfeit Currency Transaction** means all cash transactions, where forged or counterfeit Indian currency notes have been used as genuine. These cash transactions should also include transactions where forgery of valuable security or documents has taken place**.**

1.8 **"Customer"** means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

1.9 **Customer Due Diligence (CDD):**

Identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'Proof of Identity' and a 'Proof of Address'. The sources of identification should be reliable and independent. The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

(a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

(b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

(c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

1.10 **"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 Company as per the provisions contained in the Act.

1.11 **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

1.12 **"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.

1.13 **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

1.14 **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the Central KYC Records Registry (CKYCR), for individuals and legal entities, as required by the relevant Rules.

1.15 **"Designated Director"-** means a person designated by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act (PMLA) and the Rules thereunder and includes:-

a) The Managing Director or a Whole-Time Director duly authorized by the Board of Directors,

b) The name, designation and address of the Designated Director shall be communicated to the Financial Intelligence Unit-India (FIU-IND).

c) A person of senior management official designated by the Company as "Designated Director" to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012. However, in no case, the Principal Officer should be nominated as the "Designated Director".

1.16 **"Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

1.17 **"Officially Valid Document" (OVD)** means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address or any other document as notified by the Central Government in consultation with the Regulator.

1.18 **"On-going Due Diligence"** - Regular monitoring of transactions in accounts to ensure that they are consistent with the Company's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

1.19 **"Politically Exposed Persons" (PEPs)** are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

1.20 **Principal Officer (PO)**

a) An official at the management level designated by the Board of Directors of the Company for overseeing and managing the KYC& AML policies and processes.
b) The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.
c) The name, designation and address of the Principal Officer shall be communicated to the Financial Intelligence Unit-India FIU-IND.

1.21 **"Senior Management"** - for the purpose of KYC compliance shall include members of the Management Committee, Designated Director, Head of Compliance, Principal Officer (PO) and his supervisor.

1.22 **"Suspicious transaction"** means a "transaction" as defined below, including an attempted
transaction, whether or not made in cash, which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve 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 not have 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.

1.23 **"Video based Customer Identification Process (V-CIP)"**: a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

5. Money Laundering and Terrorist Financing Risk Assessment by the Company:

a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. as applicable from time to time.

b) The assessment process shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.

c) The risk assessment by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. The periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the Company to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However risk assessment should be reviewed at least annually.

d) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

6. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. The Company shall implement Customer Due Diligence (CDD) programme pertaining to ML/TF risks identified and the size of the business. Further, the Company shall monitor the implementation of the controls and enhance them If necessary.

7. Customer Acceptance Policy

In line with the Reserve Bank of India (RBI) Directions, the Prevention of Money Laundering Act (PMLA) and the Rules thereunder, the Company has formulated Customer Acceptance Policy (CAP) which lays down the broad criteria for acceptance of customers.

The features of the Customer Acceptance Policy (CAP) are detailed below:

a) The Company shall not open any account(s) in anonymous, fictitious or 'benami' name(s).

b) No account will be opened where the Company is unable to apply appropriate due diligence measures, either due to non-cooperation of the customer or non-reliability of the

documents/information furnished by the customer. The Company shall consider filing an STR if necessary when it is unable to comply with the relevant CDD measures in relation to the customer.

c) No transaction or account-based relationship shall be undertaken without following the due diligence procedure.

d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation shall be specified.

e) 'Optional'/additional information, will be obtained with the explicit consent of the customer after the account is opened.

f) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

g) CDD Procedure will be followed for all the joint account holders, while opening a joint account.

h) The Company shall ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. For this purpose, the Company shall maintain lists of individuals or entities issued by Reserve Bank of India (RBI), United Nations Security Council, other regulatory & enforcement agencies, internal lists as the Company may decide from time to time. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be treated as suspicious and reported to FIU.

i) Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate due diligence.

j) The Company may rely on third party verification subject to the conditions prescribed by Reserve Bank of India (RBI) in this regard.

k) For non-face-to-face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised for identification and verification of such customers.

l) The purpose of commencing the relationship/opening of accounts shall be established and the beneficiary of the relationship/account shall also be identified.

m) The information collected from the customer shall be kept confidential.

n) Appropriate Enhanced Due Diligence (EDD) measures shall be adopted for high risk customers from AML perspective, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically

Exposed Persons (PEPs) and their family members/close relatives.

o) Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship. However, the decision to close an existing account shall be taken at a reasonably senior level, after giving due notice to the customer explaining the reasons for such a decision.

p) Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

q) Where GST number is available, the same shall be verified through the search/verification facility provided by the issuing authority.

r) The Company shall not deny financial facilities to any members of the general public, especially to those who are financially or socially disadvantaged, including Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned.[1]

Where the Company is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR.

The Company may undertake live V-CIP, to be carried out by an official of the Company, for establishment of an account-based relationship with an individual customer, after obtaining his informed consent:

i) The Company 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.

ii) Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India.

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

iv) The official shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

v) 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 3 working days from the date of carrying out V-CIP.

vi) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

vii) The Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio- visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. The

[1] Reserve Bank of India (Know Your Customer (KYC)) (2nd Amendment) Directions, 2025 dated August 14, 2025.

Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

viii) To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

ix) The activity log along with the credentials of the official performing the V-CIP shall be preserved and

x) The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xi) The Company shall ensure to redact or blackout the Aadhar Number obtained from the client.

8. Risk Management

For Risk Management, the Company shall have a risk-based approach which includes the following:

a) Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.
b) Broad principles may be laid down by the Company for risk-categorization of customers.
c) Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
d) The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

9. List of Customer Identification Documents

Following documents are collected for customer identification and address verification:

1. Filling of KYC form and First Primary KYC document: Aadhar ID should be necessary ID for all loan disbursed for both borrower and co-borrower.

2. Second (secondary) KYC document:

    - Voter ID issued by Election Commission
    - Ration Card (only if the borrower name is mentioned on the ration card)
    - Driver License (Not expired)
    - PAN Card or Form 60
    - Job card issued to the borrower by the state government under MNREGA
    - Nationalized Banks passbook with Photo ID.
    - Utility Bill – Electricity (not more than 2 months old)

3. Bank Passbook copy of borrower or co –borrower (not more than 6 months old) along with their Photo ID.

10. Customer Identification Procedures

The Company shall undertake identification of customers in the following cases:

1. Commencement of an account-based relationship with the customer.
2. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
3. Selling their own products, selling third party products as agents and any other product for more than Rs.50,000/-.
4. Carrying out transactions for a non-account-based customer (walk-in customer).where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected;
5. The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc.
6. The Company shall obtain and verify Permanent account number (PAN) of customers as per the applicable provisions of Income Tax Rule 114B. Form 60 shall be obtained from persons who do not have PAN.
7. The documents to be accepted by the Company for customer identification shall be based on the regulatory prescriptions from time to time and shall be finalized after approval from Operations Head.
8. Decision-making functions of determining compliance with KYC norms shall not be outsourced.
9. The customers shall not be required to furnish an additional Officially valid document (OVD), if the Officially valid document (OVD) submitted for KYC contains proof of identity as well as proof of address.
10. The customers shall not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence shall be made by the Company.
11. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as cheque books, ATM cards, telephonic conversation, positive address verification etc.
12. In case of change in the address mentioned on the 'proof of address', fresh proof of address should be obtained within a period of 6 months.

11. Customer Due Diligence (CDD) Procedure

i. The Company shall obtain the following documents from an individual while establishing an account-based relationship:

a) one certified copy of an (OVD) as defined above containing details of identity and address.

b) one recent photograph; and

c) the KYC Identifier with an explicit consent to download records from CKYCR;
KYC documents downloaded from the CKYCR, but whose validity has lapsed, are not to be used for KYC purpose such other documents pertaining to the nature of business or financial status specified by the Company.

Further, the Company shall carry out authentication of the Customer's Aadhar Number using e-KYC authentication facilities provided by the Unique Identification Authority of India. Moreover, where the customer has submitted an equivalent e document of any Officially valid document (OVD), the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and rules made thereunder and take a live photo as specified in Reserve Bank of India (RBI) Circular.

ii. The information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross-selling, or for any other purpose without the express permission of the customer.

iii. A copy of the marriage certificate issued by the State Government or Gazette notification indicating change in name together with a certified copy of the 'officially valid document' in the existing name of the person shall be obtained for proof of address and identity, while establishing an account-based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise.

iv. If an existing KYC compliant customer of the Company desires to open another account with it, there shall be no need for a fresh CDD exercise provided there is no change in details last provided under the Company's KYC norms.

12. CDD Measures for Identification of Beneficial Owner (BO):

For opening an account of a Legal Person who is not a natural person, the Beneficial Owner(s) shall be identified and all reasonable steps in terms of Rule 9(3) of the PMLA Rules to verify his/her identity shall be undertaken keeping in view the following:

(i) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) 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 entities.

(ii) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

13. Combating Financial Terrorism

A. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

a. The Company shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

i. The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at **www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list.**

ii. The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011)**,** which includes names of individuals and entities associated with the Taliban is available at **https://www.un.org/securitycouncil/sanctions/1988/materials**.

b. The Company shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

c. Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021.

d. **Freezing of Assets under section 51A of UAPA, 1967:** The procedure laid down in the UAPA Order dated February 2, 2021, shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

B. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

i. Company shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 01, 2023, by the Ministry of Finance, Government of India (Annex III of the KYC Master Direction).

ii. Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

iii. Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

iv. Company shall refer to the designated list, as amended from time to time, available on the portal of FIU-India.

v. In case of match in the above cases, company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005.

A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI.

vi. In case of doubt, company shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

vii. In case an order to freeze assets under Section 12A is received by the company from the CNO, Company shall, without delay, take necessary action to comply with the Order.

viii. The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

C. Company shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-C. DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

D. In addition to the above, Company shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of section 51A of the UAPA and section 12A of the WMD Act.

E. Company shall undertake counter measures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

14. Digital KYC Process

A. The Company 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 its authenticated application.

B. The access of the Application shall be controlled by the Company 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 the Company to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the Company or vice- versa. The original Officially valid document (OVD) shall be in possession of the customer.

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

D. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color and no other person shall come into the frame while capturing the live photograph of the customer.

E. Similarly, the live photograph of the original Officially valid document (OVD) 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. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

F. Once the abovementioned 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 customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer 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 of the Company shall not be used for customer signature.

G. The authorized officer shall provide a declaration about the capturing of the live photograph of customer 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 Company. 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.

H. The authorized officer of the Company 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 customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.

15. On Successful verification, the CAF shall be digitally signed by authorized officer of the Company 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.

16. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

17. Periodic KYC Updation[2]

The Company shall ensure that periodic updation of KYC is carried out for all customers as per risk categorization and the timelines prescribed under the RBI Master Direction – KYC, 2016, as amended from time to time.

The Company may also update customer's KYC information/records based on the update notification received from CKYCR, provided requisite consent as prescribed is available with the Company.

KYC identifier as provided by CKYCR shall be the first reference point for the purpose of establishing an account-based relationship or verification of identity of Customers. Such option should be provided to the customers at the time of onboarding.

Customer may be onboarded in face to face mode through Aadhar biometrics-based e-KYC authentication and, in such cases, if the customer address, different from the address as per the identity information available in the UIDAI database (i.e. Central Identities Data Repository), the same shall be permitted post submission of self-declaration for such address by the Customer, if customers wants to. The Company shall perform all actions/activities who undertake periodic updation exercise as stipulated under the Reserve Bank of India (Know Your Customer (KYC)) (Amendment) Directions, 2025 dated June 12, 2025.

18. Reporting to Financial Intelligence Unit – India

17.1. In accordance with the requirements under Prevention of Money Laundering Act (PMLA), the Company shall furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU- IND):

a) **Cash transaction report (CTR)/Counterfeit Currency Report (CCR) –** All such cash transactions where forged or counterfeit Indian currency notes of bank notes have been used as genuine as Counterfeit Currency Report (CCR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.

[2] Reserve Bank of India (Know Your Customer (KYC)) (Amendment) Directions, 2025 dated June 12, 2025.

b) **Suspicious Transactions Reporting (STR)-** The Company shall endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to Financial Intelligence Unit-India (FIU-IND).

The Company shall file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

17.2. Confidentiality and Prohibition against disclosing Suspicious Activity Investigations and Reports-

The Company shall maintain utmost confidentiality in investigating suspicious activities and while reporting Counterfeit Currency Report (CCR)/ Suspicious Transactions Report (STR) to the Financial Intelligence Unit-India (FIU-IND)/ higher authorities. However, the Company may share the information pertaining to the customers with the statutory/ regulatory bodies and other organizations such as banks, credit bureaus, income tax authorities, local government authorities etc.

19. <u>Sharing KYC information with Central KYC Records Registry</u>

The Company shall capture the KYC information for sharing with the Central KYC Records Registry (C-KYCR) in the manner as prescribed in the Rules as per the prescribed KYC templates for 'individuals' and 'Legal Entities' as applicable. Further, the Company shall upload the KYC data pertaining to all types of prescribed accounts with Central KYC Records Registry (CKYCR), Within 10 days of commencement of an account-based relationship with the customer. as per the Operational Guidelines for uploading the KYC data issued CERSAI.

20. <u>Unique Customer Identification Code:</u>

The Company shall allot an Unique Customer Identification Code (UCIC) while entering into new relationships with Individual customers as also the existing customers of the Company.

21. <u>Independent Evaluation</u>

To provide reasonable assurance that its KYC and AML procedures are functioning effectively, an audit of its KYC and AML processes will covered under Internal Audit of the Company. The audit findings and compliance thereof will be put up before the Audit Committee of the Board on quarterly intervals.

22. <u>Responsibilities of Senior Management</u>

21.1. Designated Director- The Company shall nominate a "Designated Director" to ensure compliance with the obligations prescribed by the Act and the Rules thereunder. The "Designated Director" can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the "Designated Director".

21.2. Principal Officer- An official (having knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business) shall be designated as the Principal Officer of the Company. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/ regulations.

23. Key Responsibilities of the Senior Management

a) Ensuring overall compliance with regulatory guidelines on KYC/ AML issued from time to time and obligations under Act and Rules.

b) Proper implementation of the company's KYC & AML policy and procedures.

24. Record Management

24.1 The Company shall introduce a system of maintaining proper record of transactions required under Prevention of Money Laundering Act (PMLA) as mentioned below:

a) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions.
b) All suspicious transactions whether or not made in cash.
c) Records pertaining to identification of the customer and his/her address; and
d) Should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

24.2 For maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules. The Company shall,

a) maintain for at least 5 years from the date of transaction between the Company and the client, both domestic and international.

b) maintain for at least 5 years from the date of transaction between the Company and the client, all necessary records of transactions so as to permit reconstruction of individual transactions, including the following:

(i) the nature of the transactions.
(ii) the amount of the transaction and the currency in which it was denominated.
(iii) the date on which the transaction was conducted, and
(iv) the parties to the transaction.

25. Hiring of Employees, their Training and Education of Customers

25.1 Hiring of Employees and Employee training- Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place. On-going employee training programme shall be put in place.

25.2 The Company shall endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

25.3 On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.

Implementation of KYC Procedures requires the Company to seek information which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. To meet such a situation, it is necessary that the customers are educated and apprised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company.

26. <u>Secrecy Obligations and Sharing of Information:</u>

(a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. the interest of the Company requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.