

POLICY ON KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML) (VERSION 7).

Version Number	Prepared by	Version Control department	Approval Date	Version Details
1	-	-	29.06.2019	Initial Policy
1	Vinay Nakashe	Assistant Vice President – Operations	17.06.2020	Amendment
2	Yash Panchal	Company Secretary and Legal	04.06.2021	Amendment
3	Yash Panchal	Company Secretary and Legal	03.06.2022	Amendment
4	Yash Panchal	Company Secretary and Legal	23.05.2023	Amendment
5	Yash Panchal	Company Secretary and Legal	15.12.2023	Amendment
6	Yash Panchal	Company Secretary and Legal	02.12.2024	Amendment
7	Yash Panchal	Company Secretary and Legal	04.06.2026	Amendment

Content of the Policy

INTRODUCTION.	3
OBJECTIVE & APPLICABILITY.....	3
DEFINITION.	4
MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT.	7
KEY ELEMENTS OF THE POLICY.	7
CUSTOMER ACCEPTANCE POLICY (CAP).	8
CUSTOMER IDENTIFICATION PROCEDURE (CIP).....	8
CUSTOMER DUE DILIGENCE PROCEDURES (CDD).	9
RISK MANAGEMENT.	20
RECORD MANAGEMENT AND RETENTION.	21
REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA.	22
UNIQUE CUSTOMER IDENTIFICATION CODE (UCIC).....	23
SELLING OF THIRD-PARTY PRODUCTS.	23
REGISTRATION OF CUSTOMER WITH DARPAN PORTAL.....	23
APPOINTMENT OF DESIGNATED DIRECTOR AND PRINCIPAL OFFICER.....	23
REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES.	23
SECRECY OBLIGATIONS AND SHARING OF INFORMATION.	25
COMPLIANCES WITH THE PROVISIONS OF FOREIGN CONTRIBUTION (REGULATION) ACT, 2010.	25
HIRING OF EMPLOYEES AND EMPLOYEE TRAINING.	26
ANNEX – I DIGITAL KYC PROCESS.....	27
ANNEX – II: VIDEO BASED KYC PROCESS (V-CIP)	29

KNOW YOUR CUSTOMER (KYC) & ANTI MONEY LAUNDERING (AML) POLICY (VERSION 7)

INTRODUCTION.

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations are prescribed nationally and internationally. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of the international financial system.

The Prevention of Money Laundering Act, 2002 (PML) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). is enacted to prevent and control money laundering and to confiscate and seize the property obtained from the laundered money.

In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transaction.

Accordingly, in compliance with the PML Act and PML Rule and Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, issued by the Government of India and RBI (as amended from time to time), This policy applies to all categories of Lending products and services offered by the Company.

OBJECTIVE & APPLICABILITY.

The primary objective is to prevent the Company from being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines mandate the Company to determine the true identity, ownership of accounts, source of funds, the nature of the customer's business, and the reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently.

Accordingly, The Board of Directors, Management and all employees shall adhere to these standards to protect the Company and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

All departments shall ensure that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies.

DEFINITION.

- 2) 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).
 - 3) Account opening/onboarding for the purposes of this KYC Policy refers to the establishment of a lending relationship, including the creation of a loan/credit account or any other customer relationship involving extension of credit.
 - 4) 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.
 - 5) Beneficial Owner (BO) shall mean where;
 - a) the customer is a company the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
 - 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 ownership of entitlement to more than 10%. of capital or profits of the partnership or who has the right to control the management or policy decision;
 - 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 ownership of or entitlement to more than 15% (fifteen) per cent. of the property or capital or profits of such association or body of individuals;
where no natural person is identified under (a) or (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; and
 - e) where the customer or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- Controlling ownership interest means ownership of or entitlement to more than 10% of shares or capital or profits of the company;*
- Control shall include the right to appoint the 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;*
- 6) Customer means a person who is engaged in a financial transaction or activity with a Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
 - 7) Certified Copy means comparing the copy of the proof of possession of Aadhaar number (where offline verification cannot be carried out) or the officially valid document produced by the customer with the original, and an authorised officer of the NBFC shall record the comparison on the copy as per the provisions

contained in the Act. Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, the NBFC may alternatively obtain the original certified copy, certified by any one of the following:

- (a) authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
 - (b) branches of overseas banks with whom Indian banks have relationships,
 - (c) Notary Public abroad,
 - (d) Court Magistrate,
 - (e) Judge,
 - (f) Indian Embassy / Consulate General in the country where the non-resident customer resides.
- 8) Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding INR. 50,000, whether conducted as a single transaction or several transactions 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.
- 9) Common Reporting Standards (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.
- 10) Designated Director means the Managing Director or a whole-time Director, duly authorized by the Board of Directors to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.
- 11) Digital KYC means the capturing a live photo of the customer and an 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 authorized officer of the Company.
- 12) 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).
- 13) 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.
- 14) Know Your Client (KYC) Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.
- 15) KYC Templates means templates prepared to facilitate collating and reporting KYC data to the CKYCR, for individuals and legal entities.
- 16) Non-face-to-face customers mean customers who open accounts without visiting the branch/offices of the NBFC or meeting the officials of NBFC.

- 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.
- Provided that,*
- (c) where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form that the Unique Identification Authority of India (UIDAI) issues.
- (d) In case the address is not updated on the OVD, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address (i) utility bill which is not more than two months old (electricity, telephone, post-paid mobile phone, piped gas, water bill); (ii) property or Municipal tax receipt; (iii) pension or family pension payment orders issued to retired employees of the Govt. department or PSUs. (iv) letter of allotment of accommodation or leave and license agreement containing the current address from employers.
- 18) Offline verification shall have 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).
- 19) On-going Due Diligence means regular monitoring of transactions in accounts to ensure that those are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds/wealth.
- 20) Person has the same meaning assigned in the Act and includes:
- an individual,
 - a Hindu undivided family,
 - a company,
 - a firm,
 - an association of persons or a body of individuals, whether incorporated or not, every artificial juridical person, not falling within any one of the above person and any agency, office, or branch owned or controlled by any of the above persons (a to f).
 - any agency, office or branch owned or controlled by any of the person (a to f).
- 21) 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.
- 22) Principal Officer means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules
- 23) 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:
- 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
 - appears to be made in circumstances of unusual or unjustified complexity; or
 - appears to not have an economic rationale or bona-fide purpose; or
 - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

- e) Transaction involving financing of the activities relating to terrorism includes transaction involving funds that the NBFC suspects are linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.
- 24) Video based Customer Identification Process (V-CIP) mean an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Company by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining an audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

All other expressions, unless defined herein, shall have the same meaning as have been assigned to them in the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 as amended from time to time.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT.

The Company will carry out Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise as and when required (at least annually) to identify, assess, and take effective measures to mitigate the money laundering and terrorist financing risk arising from the customer, clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The risk assessment should be commensurate to nature, size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment approach takes cognizance of the overall sector-specific vulnerabilities, if any, which the regulator may share from time to time.

The Company should place the outcome of the assessment before the Board. The Company should apply Risk Based Approach (RBA) for mitigation and management of identified risks and shall monitor the implementation of the controls and if required enhance the controls.

KEY ELEMENTS OF THE POLICY.

The Company is hereunder framing the KYC policy incorporating the following four key elements:

- a) Customer Acceptance Policy (“CAP”);
- b) Customer Identification Procedures (“CIP”);
- c) Customer Due Diligence (CDD);
- d) Risk Management and Monitoring of Transactions

CUSTOMER ACCEPTANCE POLICY (CAP).

The company shall follow the following norms while accepting, dealing and taking the decision to grant credit facility to customers.

Provided that the Company will ensure the norms defined hereunder does not explicitly result in denial of credit facility to customers especially those who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). The Company shall record the reason of rejection of any customer not onboarded does not fall within the policy.

- a) not open an account in an anonymous/fictitious/benami name or where the Company is unable to do customer due diligence (CDD) on account of non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer.
- b) not sanctioned any credit facility to minors nor minor will be part of the credit guarantee.
- c) carry out full-scale customer due diligence (CDD) for all customers before granting credit facilities and financial products/services.
- d) obtain mandatory KYC documents as specified in the policy and other information while onboarding and during the periodic updation of the account.
- e) obtained explicit consent, if required for taking optional/additional information from the customers as per the Company risk assessment and KYC guidelines issued by the Government of India or the RBI from time to time.
- f) undertake the CDD procedure for all new applicants and guarantors at the Unique Customer Identification Code (UCIC) level. Fresh CDD procedure is not required for an existing KYC compliant customer.
- g) Place a suitable system to match the identity of the customer with the negative list of persons or entities issued by the various statutory bodies and government from time to time.
- h) may permit any other person /entity to act on behalf of the customer as per circumstances, if any.
- i) verify the PAN from the NSDL or any other authority which is authorised to issue PAN and verify the digital signature where the customer has provided an equivalent e-document to the Company.
- j) verify the GST number and GST details from the GST portal using the search/verification facility.
- k) file suspicious Transaction Reporting (STR), if necessary, with FIUIND, where the customer identity is unknown or suspicious or where, CDD procedures is not complied or not possible to process due to non-cooperation, or non-reliability of the documents produced by the customer to the Company.
- l) Photocopies of documents submitted by the customer shall be compulsorily verified with original, with signature/confirmation of the person verifying it shall be put as proof verification.

CUSTOMER IDENTIFICATION PROCEDURE (CIP).

Customer identification means identifying the customer and verifying their identity by using reliable and independent sources of documents, data or information to ensure that the customer to be onboarded is not a fictitious person. The Company will undertake CIP in the following cases:

- a) before onboarding the customer.

- b) when there is a doubt about the authenticity or adequacy of identification data already obtained.
- c) while selling own and third-party products as agent and any other product for more than Rs. 50,000 and where the customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000.

For the following limited purpose (i) verifying the identity of customers at the time of commencement of an account-based relationship (ii) carrying out an occasional transaction of an amount equal to or exceeding ₹50,000 the Company may rely on the due diligence done by a third party subject to the following conditions that;

- a) the Company shall immediately obtain CDD records and information from the third party or from the CKYC.
- b) Copies of data, documents, and information will be made available upon request without delay.
- c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- d) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

CUSTOMER DUE DILIGENCE PROCEDURES (CDD).

The company shall obtain the following documents or equivalent e-documents from the customer for conducting identification and due diligence. As part of the Loan documents, the company takes consent under the loan documentation to retrieve, verify and report the KYC information with the regulators.

1.1 The List of Documents to be collected and CDD measure performed for different type of customer are as follow;

Sr. No	Type of Customer	Type of Documents or the equivalent e-documents to be collected from the customer for Identification and address proof.
1.	Individual, (Beneficial Owner, Authorised signatory and the power of Attorney Holder related to Legal entity).	Any two of the following documents (PAN is mandatory). <ul style="list-style-type: none"> ➤ PAN Card/Form 60 ➤ Aadhaar Card/Aadhaar Number ➤ KYC Identifier with an explicit consent to download records from CKYCR ➤ Passport ➤ Voter's Identity Card issued by Election Commission ➤ Driving License ➤ job card issued by NREGA duly signed by an officer of the State Government and a Letter issued by the National Population Register containing details of name and address.

Sr. No	Type of Customer	Type of Documents or the equivalent e-documents to be collected from the customer for Identification and address proof.
		<ul style="list-style-type: none"> ➤ such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents <p>Where the above-mentioned documents do not have updated address, the Company shall take for the limited purpose of proof of address:</p> <ul style="list-style-type: none"> ➤ utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ➤ property or Municipal tax receipt; ➤ pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; ➤ letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation.
2.	Sole Proprietary firms	<p>In addition to the documents mentioned in point no. 1, any two of the following documents as Proof of business/ activity:</p> <ul style="list-style-type: none"> ➤ Registration certificate including Udyam Registration Certificate (URC) issued by the Government. ➤ Certificate/license issued by the municipal authorities under the Shop and Establishment Act. ➤ Sales and income tax returns. ➤ CST/VAT/ GST certificate (provisional/final). ➤ Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. ➤ IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. ➤ Complete Income Tax Return (not just the acknowledgment) in the name of the sole proprietor where the firm's income is

Sr. No	Type of Customer	Type of Documents or the equivalent e-documents to be collected from the customer for Identification and address proof.
		<p>reflected, duly authenticated/acknowledged by the Income Tax authorities.</p> <ul style="list-style-type: none"> ➤ Utility bills such as electricity, water, landline telephone bills, etc. <p>The Company may, at their discretion, accept only one of those documents as proof of business/activity and such other documents in respect of the nature of business and financial status of an entity.</p>
3.	Partnership Firm	<p>In addition to the documents mentioned in point no. 1, relating to beneficial owners, managers, officers, or employees or authorized signatories or holders of PoA to transact on its behalf. Certified copy of all the below documents;</p> <ul style="list-style-type: none"> ➤ Registration certificate ➤ Partnership deed, if any ➤ PAN Card/Form 60. ➤ Name of all partners ➤ Proof of address of the Registered office and Principal Place of business, if both are different. ➤ Business activity proof (as mentioned in point no. 2) ➤ Such other documents in respect of the nature of business and financial status of an entity.
4.	Legal Entity	<p>In addition to the documents mentioned in point no. 1, relating to beneficial owner, managers, officers or employees, or authorized signatories or holders of PoA to transact on its behalf. Certified copy (by Director/CS/CFO) of all the below documents;</p> <ul style="list-style-type: none"> ➤ Certificate of incorporation ➤ Memorandum and Articles of Association (MoA and AoA) ➤ PAN Card/Form 60 ➤ A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf ➤ Name of Persons holding Senior Management position ➤ Registered office and Principal place of business if both are different. ➤ Such other documents in respect of the nature of business and financial status of an entity.
5.	Trust	<p>In addition to the documents mentioned in point no. 1, relating to trustees, managers, officers or employees, beneficial owner or</p>

Sr. No	Type of Customer	Type of Documents or the equivalent e-documents to be collected from the customer for Identification and address proof.
		authorized signatories or holders of PoA to transact on its behalf. Certified copy of all the below documents; <ul style="list-style-type: none"> ➤ Registration certificate ➤ Trust deed ➤ PAN Card or Form 60. ➤ List of beneficiaries, trustees, settlor, protector, if any and authors of the trust. ➤ the address of the registered office of the trust; ➤ Such other documents in respect of the nature of business and financial status of an entity. ➤ Declaration from Trustee regarding their status while carry out each transaction.
6.	Unincorporated Association/ Unregistered trusts/partnership firms or a body of individuals	In addition to the documents mentioned in point no. 1, relating to beneficial owner, managers, officers or employees, or authorized signatories or holders of PoA to transact on its behalf; <ul style="list-style-type: none"> ➤ Resolution of the managing body of such association or body of individuals ➤ PAN Card or Form 60. ➤ Power of attorney granted to transact on its behalf and PAN of the persons holding an attorney to transact on its behalf and any OVD for identity and address proof and one recent photograph of such persons. ➤ Such other documents in respect of the nature of business and financial status of an entity.
7.	Person purports to act on behalf of juridical person or individual or trust. Specifically, not covered such as societies, universities and local bodies like village panchayats	Certified copy of all the below documents or the equivalent e-documents thereof; <ul style="list-style-type: none"> ➤ Document showing the name of the person authorised to act on behalf of the entity; ➤ Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and ➤ Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person. ➤ Such other documents in respect of the nature of business and financial status of an entity

The company may accept such other documents from the customer in addition to the above-mentioned documents to satisfy and establish the legal existence of such an entity/person. Such a list of documents shall be approved by the Head of -Operations.

1.2 Customer Due Diligence (CDD in case of the Individual, Beneficial Owner, Authorized Signatory and the Power of Attorney Holder.

Sr. No	Name of Documents or equivalent e-documents	Type of Verification/Authentication
1.	Permanent Account Number	Verify the PAN details with the issuing authority
2.	Submission and Proof of possession of Aadhaar number where offline verification can be carried out.	The Company shall carry out offline verification as per Section 8A of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
3.	Where offline verification cannot be performed; Proof of possession of Aadhaar Number, PAN, Passport, Driving Licence, Voter's Identity Card, Job card issued by NREGA, Letter issued by the National Population Register ("OVD")	The Company shall carry out verification through Digital KYC as specified under Annex I .
4.	Any equivalent e-document of any OVD containing the details of identity and address.	The Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I (Digital KYC) .
5.	KYC Identifier	The Company shall retrieve and download the KYC records and information online from the CKYCR with explicit consent of the customer as per paragraph 8.3 of the policy.

1.3 CDD Procedure and Sharing KYC Information with Central KYC Records Registry (CKYCR).

- a) The Company will capture customer KYC records and upload on the CKYCR portal within 10 days of the onboarding the customer as per KYC templates for 'Individuals' and 'Legal Entities' (LEs) issued by CERSAI from time to time.
- b) Once the KYC Identifier is generated by CKYCR, the Company will communicate the same to the individual/LE.
- c) In case the customer submit the KYC Identifier for establishing an account-based relationship then the Company will obtain explicit consent from the customer to download/retrieve records from the CKYCR using the KYC identifier.
- d) The customer will not be required to submit the same KYC record or information unless;
 - there is a change in the information of the customer as existing in the records of CKYCR;
 - the current address of the customer is required to be verified;

- the validity period of documents downloaded from CKYCR has lapsed;
 - the Company considers it necessary to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer; and
 - the KYC record or information retrieved is incomplete or is not applicable as per KYC policy.
- e) The Company shall update any additional information or document if any received from the existing customers within 7 days in CKYCR records. Once CKYCR informs the Company regarding an update in the KYC record of an existing customer, the Company shall retrieve the updated KYC records from CKYCR and update the KYC record.
- f) For establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, the Company may obtain KYC Identifier from the customer or retrieve the KYC Identifier and proceed to obtain KYC records online by using such KYC Identifier unless:
- there is a change in the information of the customer as existing in the records of CKYCR; or
 - the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
 - the validity period of downloaded documents has lapsed; or

the Company considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

1.4 Identification of Beneficial Ownership (BO).

Before onboarding a customer, who is not a natural person (i.e., non-individual), the Company shall identify the beneficial owner(s) and verify the beneficial owner's identity.

Nature of Customer	Beneficial Owner of the Entity	
Company	Natural person who, whether acting alone or together, or through one or more Person purports to act on behalf of a juridical person or individual having controlling ownership interest or who exercise control through other means.	Controlling ownership interest” means ownership of or entitlement to more than 10% of shares or capital or profits of the company; “Control” shall include the right to appoint the 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;
Partnership Firm	Natural person who, whether acting alone or together, or through one or more Person purports to act on behalf of a juridical person have ownership or entitlement or who exercises control through other means.	Ownership of entitlement to more than 10% of capital or profits of the partnership;

Nature of Customer	Beneficial Owner of the Entity	
Unincorporated Association or Body of Individuals	Natural person who, whether acting alone or together, or through one or more judicial person have ownership or entitlement of unincorporated association or body of individual	Ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals
Trust	Natural person exercising ultimate effective control over the trust through a chain of control or ownership	Trust, Trustee or beneficiaries having 10% or more interest.
where no natural person is identified	the beneficial owner is the relevant natural person who holds the position of Senior Management officials;	
Where the customer the beneficial owner is an entity listed on a stock exchange or it is a subsidiary of such listed entities or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions	it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.	

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 shall be obtained.

1.5 In case the customer is not able to produce documents as mentioned in the Para 8 the Company may onboard the customer subject to the following conditions [Simplified procedure for opening of accounts].

- a) The Company will obtain a self-attested photograph from the customer.
- b) The designated officer of the Company has to certify under his signature that the person onboarded has affixed his signature or thumb impression in his presence.
- c) The account shall remain operational initially for a period of 12 months, within which full KYC and CDD shall be performed by the Company.
- d) The total credit in all the accounts taken together shall not exceed INR. 1 Lakh in a year and shall be made aware to do a full KYC account. In case the account is not fully KYC complied no further transaction is allowed in the account.

- e) The customer shall be notified when the total credit in a year reaches INR. 80,000 that appropriate documents for conducting the KYC to be submitted otherwise no further credit will be provided and the account shall be stopped.
- f) KYC verification once done by one branch/office of the Company shall be valid unless its not due for periodic updation.

The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be as per CDD procedure.

1.6 Accounts Opened using Aadhaar OTP based E-KYC in Non-Face-To-Face shall be subject to the following conditions.

- a) The Company will obtain specific consent before onboarding the customers through an Aadhaar registered number only.
- b) As risk mitigating measure for an Aadhaar OTP based account, the transaction alerts, OTP, etc., will be sent only to the registered mobile number associated with the Aadhaar card. The customer shall not be allowed to change the mobile number unless the mobile number is registered with Aadhaar.
- c) Only term loans will be sanctioned to the customer which shall not exceed INR. 60,000 in the financial year.
- d) The customer onboarded using OTP based e-KYC will be operative for 1 year unless the full KYC and due diligence is performed. If Aadhaar details are used in the process then it shall be followed in its entirety including authentication through fresh Aadhaar OTP.
- e) In case full KYC and CDD procedure is not performed within the year the Company shall not sanction or renewed or further disbursed the loan in the account.
- f) The Company shall ensure that application shall include onetime declaration to the effect that “customer confirmed that it has not opened or will not open other account using OTP based KYC in non-face-to-face mode”. The Company will indicate in the CKYCR that accounts are opened using OTP based e-KYC and other RE shall not rely upon the KYC information and open the account.
- g) Company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

1.7 V-CIP.

The Company may opt to undertake customer, authorized signatory and beneficial owners due diligence using V-CIP as per Annex- II for onboarding new customers, conversion of existing accounts opened in non-face to face mode or by using Aadhaar OTP based e-KYC authentication and updation of KYC information’s for eligible customers;

1.8 On-Going Due Diligence/Updation/Periodic Updation of KYC.

The Company will adopt a risk-based approach for ongoing due diligence/periodic updation of KYC of the customer. The company will ensure that the information, and data collected under CDD measure and KYC shall be kept up to date as per risk categorization.

The ongoing due diligence of customers shall include customers' business and risk profile, and the source of funds/wealth to ensure that their accounts are consistent with their knowledge about the customers.

The Company shall necessarily monitor the following types of transactions;

- Those transactions with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- Transactions which exceed the thresholds, if any internally prescribed for specific categories of accounts.
- Repayment from third party accounts.

A periodic review of risk categorization of accounts shall be done at least half yearly for application for enhanced due diligence measures. The Company may consider obtaining a recent photograph, requirement for physical presence of the customer, requirement of periodic updation of KYC only in the branch where the credit facility is obtained or a more frequent periodicity of KYC updating than the minimum specified in the policy. Also, the high-risk accounts should be more intensively monitored.

The periodic updation will be carried out at least once in every two years for high-risk customers, once in every eight years for medium-risk customers and once every ten years for low-risk customers.

Entity	Criteria	Documents for periodic updation.
Individual Customers	No change in KYC information	a self-declaration will be obtained through a registered email ID, mobile number, or letter in this regard.
	Change in address	a self-declaration of the new address will be obtained through a registered email ID, mobile number or letter and the declared address shall be verified through positive confirmation within two months, by means such as an address verification letter, contact point verification, deliverables etc. or a copy of OVD or the equivalent e-documents thereof for the purpose of proof of address
		Aadhaar OTP based e-KYC in non-face to face mode may be used for updation/periodic updation. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.
Other than Individual	No change in KYC information	a self-declaration will be obtained through a registered email ID, letter from an official authorised along with a Board resolution. The Company shall also obtain fresh Beneficial Owner (BO) information and update the record.

Entity	Criteria	Documents for periodic updation.
	Change in KYC information	The company shall undertake the KYC process equivalent to that applicable for onboarding a new customer.

In addition to the above, the Company shall ensure that:

- a) If KYC documents are not as per the current CDD standard, then the KYC documents of the customer as per the current CDD standards shall be obtained, even if there is no change in the customer information.
- b) PAN details shall be verified from the database of the issuing authority at the time of periodic updation of KYC
- c) The Company shall provide an acknowledgment for receipt of any documents/letter for KYC updation and the record shall be promptly updated in the system mentioning the date of KYC updation.
- d) The customer can provide their updated KYC information directly with our Branches or at the central office with the Operation Department.
- e) The Company shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit to the Company the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at the Company's end.
- f) The Company shall ensure it will inform the customer in advance, wherever possible to update their KYC. Prior to the due date of periodic updation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options / channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations.

1.9 Enhanced And Simplified Due Diligence.

The Company is primarily engaged in MSME finance. It does not deal with such a category of customers who could pose a potentially high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company also does not open account or provide credit facilities to minors.

1.10 For non-face-to-face customer onboarding (other than customer onboarding using Aadhar OTP base account).

The non-face-to-face customer onboarded by the Company (i.e. the customer without meeting the customer physically or through V-CIP). This includes the use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining a copy of OVD certified by additional certifying authorities. Following EDD measures shall be undertaken by the Company for non-face-to-face customer:

- a) The Company shall at first option provide a V-CIP facility if introduced for onboarding the remote customer.
- b) In order to prevent fraud, the Company shall not link alternate mobile numbers post CDD with such accounts for transaction OTP, transaction updates, etc. Any revision or new application of credit facility shall be permitted only from the mobile number used for onboarding.
- c) Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before onboarding or operations in the account. Positive confirmation may be carried out by means such as an address verification letter, contact point verification, deliverables, etc.
- d) The Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from the existing KYC-complied bank account of the customer.
- f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in a face-to-face manner or through V-CIP.

1.11 Accounts of Politically Exposed Persons (PEPs).

The Company business model of lending to MSME borrowers, the Company does not ordinarily expect to onboard the customers or beneficial owners who qualify as PEP including foreign PEPs, However, recognising that PEP classification under the RBI guidelines includes domestic and foreign PEPs, the Company shall identify and screen customers and Beneficial Owners who are or have been entrusted with prominent public functions, including but not limited to senior politicians, senior government, judicial or military officers, senior executives of state-owned corporations, and important political party officials.

If the customer or beneficial owner (including family members and close associates) is a Politically Exposed Person, the Company shall perform additional due diligence measures as mentioned below;

- a) The Company shall take additional information and documents concerning to the source of funds and wealth of the PEP and its relative.
- b) Any sanction to grant a credit facility to PEP shall be approved by the Board of Directors only.
- c) Sufficient information including information about the sources of funds and accounts of family members and close relatives is undertaken wherever possible;
- d) all PEP accounts will be subjected to enhanced monitoring on an ongoing basis;
- e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, committee or board level approval is obtained to continue the business relationship.

1.12 Accounts Opened by Professional Intermediaries.

The Company shall ensure while onboarding the customers through third party professional intermediaries that:

- a) The Company shall identify customer when a professional intermediary opens a account on behalf of a single client

- b) The Company shall not onboard the customer of such professional intermediaries who are bound by any client confidentiality which prohibits disclosure of the customers details.
- c) The Company shall identify all the beneficial owners where intermediaries do not co-mingle funds at the level of the NBFC, and there are 'sub- accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of the NBFC, the NBFC shall look for the beneficial owners.
- d) The Company may rely on the CDD procedure of the regulated professional intermediaries.

RISK MANAGEMENT.

The Company will follow a Risk based approach for doing customer assessments. The Company is serving to MSME sector and provides various types of credit facilities and services.

The risk categorization i.e low, medium and high will be based on the following parameters:

- a) Customer’s identity;
- b) Social/financial status;
- c) Nature of business activity;
- d) business information and their location;
- e) geographical risk covering customers as well as transactions;
- f) type of products/services offered;
- g) delivery channel used for delivery of products/services;
- h) types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, and
- i) Ability of the customers to confirm identity documents through online or other services offered by issuing authorities.
- j) Customer’s identity: the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

Indicative List of Risk Categorization

Low Risk	<p>Individuals and entities whose identities and sources of income/fund can be easily identified. The MSME enterprise is entities of modest mean and lies at the bottom of the economy or into the non-formal sector. Most of their turnover might be conducted in cash. However, for PML and AML purview the same shall be categorized as low risk due to the small aggregate transaction.</p> <ul style="list-style-type: none"> ➤ Low risk customers includes the customers or entities operating in industry segments not mentioned under the negative list/caution profiles as per the credit policy.
Medium Risk	<p>Customers who are likely to pose a higher-than-average risk may be categorized as a medium or high risk depending on the customer's background, nature and location of the activity, country of origin, sources of funds and customer profile, etc.</p>

	<ul style="list-style-type: none"> ➤ Medium-risk customers Low risk customers include the customers or entities are listed in the negative list/caution list profile as per credit policy.
Hight Risk	<p>Customers who are likely to pose high risk require a higher level of monitoring due to their customer profile or the nature of their business or the location of such customer.</p> <p>The non-face-to-face to face customers,</p> <ul style="list-style-type: none"> ➤ Non-profit Organization or Section 8 Companies ➤ Politically Exposed Person. ➤ Persons having dubious reputation as per public information available, etc. ➤ Firms with 'sleeping partners, ➤ Customers requesting for frequent change of address/contact details ➤ Sudden change in the loan account activity of the customers ➤ Frequent closure and opening of loan accounts by the customers ➤ Negative list issue by RBI, Government and Internal Agency <p>The Company shall undertake ongoing due diligence and monitoring of high-risk customers to ensure that their transactions are consistent with Company knowledge.</p>

RECORD MANAGEMENT AND RETENTION.

The Company shall take the following steps regarding maintenance, preservation, and reporting of customer account information, regarding provisions of the PML Act and Rules:

- a) The Company shall maintain all records of the transaction between the Company and the customer for at least 5 years from the date of the transaction.
- b) The company shall preserve the identification/address documents of the customer for a period of 5 years after the business relationship is ended.
- c) The Company will evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.
- d) The Company shall maintain all the information and a record of transactions as prescribed under the Prevention of Money Laundering Rule 3 including the following:
 - the nature of the transactions;
 - the amount of the transaction and the currency in which it was denominated;
 - the date on which the transaction was conducted; and
 - the parties to the transaction.
- e) The Company shall maintain records of the identity and address of its customers, and records in respect of transactions referred to in Rule 3 in hard or soft format.
- f) The Company shall evolve its internal systems for proper maintenance and preservation of account information in such manner to ensure that data and information retrieve easily and quickly.

1.13 Maintenance of records of transactions (nature and value) as per Rule 3 of PML (Maintenance of Records)**Rules 2005:**

- a) All cash transactions of the value of more than Rs.10 lakhs or its equivalent in foreign currency.
- b) All series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rs.10 lakhs or its equivalent in foreign currency.
- c) All transactions involving receipts by non-profit organizations of value more than Rs. 10 lakh, or its equivalent in foreign currency
- d) 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 has taken place.
- e) All suspicious transactions whether or not made in cash.
- f) all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of the fund is in India;
- g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.
- h) Receipt of Rs. 2 Lakhs or more in cash from a person in a single day or in respect to single transactions as per section 269ST of Income Tax, 1961.

The Company shall maintain records of the identity and address of their customer, and records in respect of the above transactions in hard or soft format.

REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA.

The Company will be furnished to the Director, Financial Intelligence Unit-India (FIU-IND), information referred in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in accordance with Rule 7 thereof.

- a) The Principal Officer of the Company will furnish the cash transaction report (CTR) in the prescribed format with respect to transaction referred clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 by 15th of every succeeding month.
- b) The Principal Officer of the Company will furnish the Suspicious Transaction Report (STR) in the prescribed format with respect to the transaction referred to in clause (D) of sub-rule (1) of PML Rule 3, Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, immediately after arriving at the conclusion that the transaction is suspicious.
- c) The Principal Officer of the Company will furnish the information in the prescribed format with respect to transaction clause (F) of sub-rule (1) of rule 3, 15th of the every succeeding the quarter.
- d) The Company shall deploy robust software which is capable (i) of throwing alerts when the transactions are inconsistent with risk categorization, (ii) updated profile of the customers will be put into use as a part of effective identification and reporting of suspicious transactions.
- e) Reporting of those accounts identified and operated as Money Mules. Money Mules accounts are those accounts which are used to launder the proceeds of fraud schemes by criminals who gain illegal access to accounts by recruiting third parties which act as “money mules.”

UNIQUE CUSTOMER IDENTIFICATION CODE (UCIC).

Every customer is provided with a unique customer ID. This helps to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the organization to have a better approach to risk profiling of customers.

SELLING OF THIRD-PARTY PRODUCTS.

The Company acting as an agent while selling third party products shall comply with the following directions;

- If the transaction value is above Rs. 50,000, the identity and address of the walk-in customer will be verified by the Company.
- The Company shall maintain complete records of the third-party product.
- The Company shall obtain and verify the PAN given by the account-based as well as walk-in customers.

REGISTRATION OF CUSTOMER WITH DARPAN PORTAL.

The Company shall ensure that in case of customers who are non-profit organisations, the Company registers details of such customers on the DARPAN Portal of NITI Aayog. If they are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of 5 years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

APPOINTMENT OF DESIGNATED DIRECTOR AND PRINCIPAL OFFICER

Mr. Pravash Dash Managing Director & CEO is the designated director who is responsible for ensuring overall compliance as required under the PML Act and the rules.

Mr. Kunal Mehta, Executive Director is designated as the Principal Officer who shall be responsible for monitoring and reporting of all transactions and sharing of information to FIU-IND.

The Company shall communicate to the FIU IND and the Reserve Bank of India if any changes the officer with name, designation, address, and contact details.

Senior Management shall be defined as per the HR policy of the Company.

REQUIREMENTS/OBLIGATIONS UNDER INTERNATIONAL AGREEMENTS - COMMUNICATIONS FROM INTERNATIONAL AGENCIES.

The Company shall ensure that it does not have any account i.e credit facility sanction in the name of individuals and entities appearing in the negative or susceptible list sanction or issued under the following Acts, Regulators, and Agencies are as under:

The Company shall ensure details of such account resembling to it shall be reported to FIU-IND including transaction details, particular of funds, financial assets, etc. The Company shall not open an account if such a name appears in the list.

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

In terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 as amended from time to time, the Company does not have any account in the name of individuals/entities which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under:

- a) The “ISIL (Da’esh) & Al-Qaida Sanctions List”, established and maintained under 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
- b) 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>

1.15 Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007.

The Company shall verify 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, on a 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.

1.16 Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 & Freezing of Assets under section 51A of UAPA, 1967.

The Company shall report the details of accounts resembling any of the individuals / entities in the lists to FIU-IND. The Company shall also strictly follow the procedure laid down in the UAPA Order dated February 2, 2021 and shall ensure the meticulous compliance with the Order issued by the Government.

1.17 Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

In case the customer’s name and entities matches the above, the 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) i.e FIU-IND, designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to the State Nodal Officer of the RBI.

1.18 UNSCR 1718 Sanctions List of Designated Individuals and Entities, as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>

1.19 Other International Laws and Regulations.

1.19.1 EU Consolidated list of persons, groups and entities subject to EU financial sanctions.:

<https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>

1.19.2 World Bank Listing of Ineligible Firms and Individuals: <https://www.worldbank.org/en/projects-operations/procurement/debarred-firms>

1.19.3 OFAC Specially Designated Nationals And Blocked Persons List and consolidated List:

<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

<https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-non-sdn-lists>

1.20 Jurisdictions that do not or insufficiently apply the FATF Recommendations:

The Company shall consider statement and information issued by the RBI in this regards from time to time and shall apply enhance due diligence to such customers.

SECRECY OBLIGATIONS AND SHARING OF INFORMATION.

- a) The Company shall maintain secrecy regarding the customer information that arises out of the contractual relationship between the Company and customers.
- b) The Information collected and obtained form the customer for purpose of onboarding the customer as confidential and shall not divulge details thereof 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 will ensure that information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions except where disclosure is under compulsion of law, there is a duty to the public to disclose, the interest of the Company requires disclosure, and the disclosure is made with the express or implied consent of the customer.

COMPLIANCES WITH THE PROVISIONS OF FOREIGN CONTRIBUTION (REGULATION) ACT, 2010.

The Company shall ensure strict compliance with the provisions of the Foreign Contribution (Regulation) Act, 2010, and the rules issued thereunder, as amended from time to time.

The Company shall also ensure compliance with all instructions, guidelines, and communications issued by the Reserve Bank of India from time to time in relation to the Foreign Contribution (Regulation) Act, 2010, including those issued pursuant to advisories or directions received from the Ministry of Home Affairs, Government of India

HIRING OF EMPLOYEES AND EMPLOYEE TRAINING.

The Company shall undertake an adequate screening mechanism as an integral part of their personnel recruitment/hiring process and conduct ongoing employee training programs that the employees are adequately trained in KYC/AML policy.

ANNEX – I DIGITAL KYC PROCESS.

The Company may undertake Customer Due Diligence (CDD) through the **Digital KYC Process**, in accordance with paragraph 24 of the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, as amended from time to time.

1. The Digital KYC (apps/software) shall be provided by the Company to its authorized employees and agents (authorized officer), if any, for the purpose of undertaking KYC of customers, and the Digital KYC process shall be carried out only through such authenticated application.
2. The Company shall control access to the Digital KYC application to prevent unauthorised use and shall ensure that the application is accessed only through controlled mechanism such as login-id and password or Live OTP or Time OTP or any other mechanism controlled by the Company.
3. For the purpose of KYC, the customer may visit the branch or authorized officer visit the customer location and review the original OVD documents of the customer.
4. The Digital KYC application shall enable capturing of live photograph of the customer by the authorized officer and the same photograph shall be embedded in the Customer Application Form (CAF). The application shall automatically embed a readable watermark on the live photograph containing CAF number, GPS coordinates, authorized official's name, unique employee code and Date (DD:MM: YYYY) and time stamp (HH:MM: SS) on the captured live photograph of the customer.
5. The application shall have the capability that only a live photograph of the customer is captured and not capture any printed or video graphed photograph. The background behind the customer while capturing the live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
6. The application shall capture only live photograph of the original OVD or proof of possession of Aadhaar and shall be placed horizontally and should be captured vertically from above and water-marking as mentioned in the point no 4 shall be apply.
7. Authorized officer shall ensure no skew or tilt in the mobile device while capturing the live photograph of the original documents.
8. The Digital KYC process shall ensure that the live photograph of the customer and image of documents are captured in proper lighting condition such that its clearly readable and identifiable.
9. The Authorized officer shall fill all entries in the CAF as per the documents and information furnished by the customer. Wherever a Quick Response (QR) code is available on the documents, the relevant details shall be auto-populated by scanning the QR code instead of manual entering of the details.
10. Upon completion of the above-mentioned process, a One Time Password (OTP) message containing the text that "Please verify the details filled in form before sharing OTP" shall be sent to the customer's own mobile number for confirmation. However, in case the customer does not have their own mobile number, the mobile number of the family member may be used for validation subject to appropriate controls by the Company.
11. The application shall ensure that the mobile number used for the customer signature does not belong to the authorized officer of the Company. In no case shall the mobile number of an authorized officers be used for customer signature.

12. Upon completion of the signature on the CAF, the application shall generate the unique transaction id/reference id number and provide the same to the customer for future reference.
13. Before submitting the CAF, the authorised officer shall verify and confirm that:
 - the information visible on the captured document images matches with the details entered in the CAF;
 - the live photograph of the customer matches with the photograph available on the document; and
 - all mandatory fields in the CAF have been correctly and completely filled.
14. After verification, the CAF shall be digitally signed by the Authorised officer and get signatures/thumb-impresion of the customer shall be obtained at the appropriate place on CAF. The signed CAF shall be uploaded into the system and original hard copy, if any, may be returned to the customer.

ANNEX – II: VIDEO BASED KYC PROCESS (V-CIP)

1. V-CIP Infrastructure

- 1.1. The application and infrastructure of the Company shall comply with the RBI guidelines on the minimum baseline cyber security and resilience framework for NBFCs, as updated from time to time, as well as other applicable guidelines relating to information technology and cyber security risks.
- 1.2. The technology infrastructure for V-CIP shall be housed in the Company own premises and the V-CIP connection and interaction should be originated from the Company own secured network domain. Any technology related outsourcing for the process should be compliant with relevant guidelines issued by the RBI from time to time. Wherever, there is cloud deployment model will be used, the Company shall ensure that the ownership of data in such model rests with the Company and all the data including video recording shall be immediately transferred to the Company exclusively owned/leased server(s) including cloud server, if any, after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider.
- 1.3. The Company infrastructure should ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.
- 1.4. The V-CIP infrastructure/application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- 1.5. The video recordings should contain the live GPS coordinates (geo-tagging) of the customer undertaking the V-CIP and the date-time stamp. The quality of the live video in the V-CIP should be adequate to allow identification of the customer beyond doubt.
- 1.6. The application should have components with face liveness/spoof detection as well as face-matching technology with a high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.
- 1.7. Based on experience of detected/attempted/'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows should be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.
- 1.8. The infrastructure should periodically undergo tests such as Vulnerability Assessment, Penetration testing, and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap identified in such test shall be timely mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of the Indian Computer Emergency Response Team (CERT-In. Such tests should also be carried out periodically in conformance to internal/regulatory guidelines.
- 1.9. The V-CIP application software and relevant APIs/webservices should also undergo appropriate testing of functional, performance, maintenance strength before being used in a live environment. Only after the closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

2. V-CIP Procedure

- 2.1. The Company should formulate a clear work flow and standard operating procedure for V-CIP. The V-CIP process should be operated only by specially trained officials of the Company. The officials shall be responsible to carry out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.
- 2.2. In case there is a disruption of any sort including pausing of video, reconnecting calls, etc., should not result in the creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop/disconnection, the application shall initiate fresh session.
- 2.3. To establish that the interactions are real-time and not pre-recorded, the sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied.
- 2.4. If any prompting is observed at the end of the customer, the application should reject the process of KYC.
- 2.5. The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at the appropriate stage of workflow.
- 2.6. The authorized official of the Company who is performing the V-CIP should record audio-video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:
 - OTP based Aadhaar e-KYC authentication
 - Offline Verification of Aadhaar for identification
 - KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer
 - Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker.
 - The application shall redact or blackout the Aadhaar number.
 - In case of offline verification of Aadhaar using an XML file or Aadhaar Secure QR Code, the Company should ensure that the XML file or QR code generation date should not be older than 3 working days from the date of carrying out V-CIP.
 - The Company should also complete the V-CIP within 3 working days of downloading/obtaining the identification information through CKYCR/Aadhaar authentication/equivalent e-document.
- 2.7. In case the address of the customer is different from that indicated in the OVD, suitable records of the current address should be captured. The Company should also ensure that the economic and financial profile/information submitted by the customer should also confirmed from the customer undertaking the V-CIP in a suitable manner.
- 2.8. Application should capture a clear image of the PAN card displayed by the customer during the process, except where e-PAN is provided by the customer. The PAN details should be verified from the database of the issuing authority including through Digilocker.

- 2.9. The Company should ensure that use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.
- 2.10. The authorized official of the Company should ensure that the photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN should match with the details provided by the customer.
- 2.11. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.

3. V-CIP Records and Data Management

- 3.1. The entire data and recordings of V-CIP should be stored in a system located in India. The Company should ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in the RBI master direction shall be equally applicable for V-CIP.
- 3.2. The activity log along with the credentials of the official performing the V-CIP shall be preserved.