AGRIWISE FINSERV LIMITED

KNOW YOUR CUSTOMER (KYC) AND ANTI MONEY LAUNDERING (AML) POLICY

Agriwise Finserv Ltd.,
Unit No 802 08th Floor Sumer Plaza
Marol Maroshi Road, Marol Naka
Andheri East, Mumbai – 400059.
Tel no.: +91-22-61829700
CIN No. – U65999MH1995PLC267097
https://www.agriwise.com/

Agriwise Finserv Limited	
Policy Title	Know Your Customer (KYC) and Anti Money Laundering (AML)Policy
Reviewing & Approving Authority	RMC/Board of Directors
Version No.	1.1
Date of approval	29th May, 2015
Date of updated Version	17th June, 2024
Review Cycle	Annually or as recommended by the Board of Directors
Nature of Document	For internal circulation & Compliance purpose only

agriwise
we give credit

TABLE OF CONTENTS

1.	*Introduction*	*4*
2.	*Definition*	*4-9*
3.	*Purpose*	*9*
4.	*Scope of the policy*	*9*
5.	*Role and Responsibilities*	*10-11*
	5.1 Designated Director	
	5.2 Principal Officer	
	5.3 Audit Committee	
	5.4 Escalation process	
6.	*Key elements of KYC*	*11-15*
	6.1 Customer Acceptance	
	6.2 Customer Identification	
	6.3 monitoring of transactions – Anti-Money Laundering	
	6.4 Risk Management	
7.	*Money Laundering and Terrorist Financing Risk Assessment*	*15*
8.	*Officially Validated Documents*	*15-17*
	8.1 e-KYC	
9.	*Customer Due Diligence*	*17-18*
	9.1 Ongoing Due Diligence	
10.	*Enhanced Due Diligence*	*18-19*
11.	*Periodic updations of KYC records*	*19-20*
	11.1 Updating of e-KYC accounts	
12.	*Record Management*	*20*
13.	*Record Management Reporting to FIU-IND*	*21-23*
14.	*Combating financing of terrorism*	*23-24*
	14.1 Transactions with jurisdictions that do not or insufficiently apply the FATF recommendations	
15.	*Issuance of UCIC*	*24*
16.	*Secrecy Obligations and Sharing of Information*	*24*
17.	*Employee training and Hiring of Employees / accountability*	*25*
18.	*Accounts of Politically Exposed Persons (PEPs) resident outside India*	*25*
19.	*Accounts of non-face-to-face customers*	*25*
20.	*Central KYC Registry (CKYCR)*	*25*
21.	*Indicative list of documents to be collected from the customers for due diligence*	*26-31*
	21.1 General guidelines for collecting the documents	
22.	*Review of Policy*	*31*
	Annexures:	
	Annex - I Digital KYC Process	*32-38*
	II Video Customer Identification Process	
	III Illustrative list of suspicious transactions:	
	(i) Builder Project / corporate clients	
	(ii) Individual	

agriwise
we give credit

1 INTRODUCTION

The Know Your Customer (KYC) and Anti Money Laundering (AML) Policy (hereinafter referred to as 'The policy' or 'Policy') has been prepared in accordance with Reserve Bank of India (RBI) Master Direction Know Your Customer' (KYC) Direction 2016 (updated as on 10th May, 2021) and obligations of NBFCs in terms of Rules notified thereunder. The policy also considers the provisions of Prevention of Money Laundering Act, 2002 and Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (and subsequent amendments thereto).

This policy supplements the existing RBI guidelines and any subsequent guidelines would over-ride this policy. Agriwise Finserv Limited (hereinafter referred to as "the company" or "AFL") is advised to follow certain norms for customer identification at the time of account opening and ongoing monitoring of the transactions; the same has covered in this policy.

One of the best methods of preventing and deterring money laundering is a sound knowledge of a customer's business and pattern of financial transactions. The adoption of procedures by which companies 'know their customer is not only a principle of good business but is also an essential tool to avoid involvement in money laundering. It is also important for the management to consider money laundering prevention and knowing their customer as a part of their risk management strategy. Thus, KYC checks and AML measures are important to prevent the company from being misused for money laundering or financing of terrorism activities.

2 DEFINITION

Definitions in these Guidelines, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below: -

(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i) **"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).

ii) **"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.

iii) **"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. iv) "Beneficial Owner" (BO):

a) Where the customer is a company, the BO 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.

For the purpose of this sub-clause: -

1) "Controlling ownership interest" means ownership of/entitlement to more than 15 per cent of the shares or capital or profits of the company.

2) "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 shareholder's agreements or voting agreements.

b) Where the customer is a partnership firm, the BO is the natural person(s), who, whether alone or together, or through one or more juridical person, has / have ownership of entitlement acting to more than 15per cent of capital or profits of the partnership.

c) Where the customer is an Unincorporated Association or 'Body of Individuals'**, the BO 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 BO is the relevant natural person who holds the position of Senior Managing Official.

d) Where the customer is a trust, the identification of BO shall include identification of the author of the trust, the trustee, the beneficiaries with 15% 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.

v.) **"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 document so produced by the customer with the original and recording the same on the copy by the authorised officer of the company as per the provisions contained in the Act.

vi.) "**Central KYC Records Registry" (CKYCR**) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vii.) **"Designated Director**" means the Managing Director or a whole-time Director, duly authorized by the Board of Directors of company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-Time Director" shall have the meaning assigned to them in the Companies Act, 2013.

viii.) **"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.

ix.) **"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).

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

xi.) **"Non-profit organisations" (NPO)** means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

xii.) **"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,

a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. where the OVD furnished by the customer does not have updated address, 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 of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. 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 licence agreements with such employers allotting official accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xiii.) **"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).

xiv.) **"Person"** has the same meaning as defined in the Act and includes: a) An individual, b) A Hindu undivided family, c) A company, d) A firm, e) An association of persons or a body of individuals, whether incorporated or not, f) Every artificial juridical person, not falling within anyone of the above persons (a to e), and g) Any agency, office or branch owned or controlled by any of the above persons (a to f).

xv.) "**Principal Officer**" means an officer nominated by the company, responsible for furnishing information as per rule 8 of the Rules.

xvi.) "**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.

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

xvii.) **"Transaction"** means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. opening of borrower's loan account;
b. deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
f. establishing or creating a legal person or legal arrangement.

xviii.) "Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of 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. Such process shall be treated as face-to-face process for the purpose of these guidelines.

xix.) "Senior Management" for the purpose of KYC Compliance:

Senior Management for the purpose of KYC compliance shall mean.

1. Designated Director, Principal Officer, Chief Compliance Officer, Chief Financial Officer, head of each department and regional business heads in the Company.
2. Senior Management shall assist the Principal Officer/Designated Director in the effective implementation of the KYC Program and submit compliance status report to them.

b.) Terms bearing meaning assigned in these guidelines, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "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.
ii. "Customer" means a person who is engaged in a financial transaction or activity with company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
iii. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.
iv. "Customer identification" means undertaking the process of CDD.
v. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
vi. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.
vii. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
viii. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/important political party officials, etc.

ix. "**Regulated Entities**" (REs) means :

a. All Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'.

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers).

e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers).

f. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

g. "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

3 PURPOSE

The purpose of the KYC and AML policy of the company is to ensure that the company understands/knows its customers and their transactions and to have a system to keep in check the money laundering activities.

The policy has been framed:

- To ensure compliance with the applicable rules and regulations;
- To obtain an understanding of the customer and transactions undertaken by them;
- To ensure that there is a customer acceptance and identification mechanism;
- To put in place appropriate controls to identify suspicious transactions and enable their timely reporting;

4 SCOPE OF THE POLICY

The provisions of KYC and AML policy shall apply to all the branches/offices of the company.

For the purpose of this policy, '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.

In terms of PML Act a 'person' includes:

i. an individual,
ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. an association of persons or a body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. any agency, office or branch owned or controlled by any of the above persons (i to vi).

5 ROLES AND RESPONSIBILITIES

The Company's Board of Directors will oversee the implementation of KYC & AML norms and the management team is responsible for implementing the KYC & AML norms hereinafter detailed, and to Ensure That Its Operations Reflect Its Initiatives to Prevent Money-Laundering Activities.

5.1 Designated Director

Company shall nominate a whole time director or the Managing Director as 'Designated Director', as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules. Further, the guidelines also allow nominating a person who holds the position of senior management or equivalent as a 'Designated Director'.

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

The role of a Designated Director is to observe the procedure and the manner of maintaining and furnishing information as specified by the regulator.

5.2 Principal Officer

Company shall appoint a senior management officer as the Principal Officer. The name, designation and address of the Principal Officer is to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

The Principal Officer shall also be responsible for timely submission of various returns to FIU-IND. Principal Officer shall report directly to the senior management/Board of Directors.

The Designated Director, in no case shall be the same as Principal Officer, and vice versa.

5.3 Audit Committee

Audit Committee of the Board & Concurrent / Internal Auditors the Audit Committee of the Board shall supervise the overall compliance with the guidelines. The scope of internal audit of the company shall also include testing of compliance with the AML / KYC Policy and procedures. Concurrent / Internal Auditors shall specifically check and verify the application of AML / KYC policy and procedures, and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board at quarterly intervals.

5.4 Escalation Process

All units / departments / offices /branches of the company shall escalate any identified suspicious activity or transaction to the Principal Officer, immediately after establishing reasonable grounds for suspicion. The Principal Officer shall report to the FIU-IND all suspicious activities / transactions in accordance with the PMLA rules, within 7 days from the date of arriving at such conclusion that any transaction, whether cash or non-cash, or a series of integrally connected transactions are of suspicious nature.

6 KEY ELEMENTS OF KYC

As set out by RBI, below are four critical elements that need to be addressed by the KYC policy of the company.

- Customer Acceptance
- Customer Identification
- Monitoring of transactions
- Risk Management

These elements are critical in establishing a strong and sound KYC & AML framework in the organization.

6.1 Customer Acceptance

At the time of on boarding the customer, the company shall ensure adherence to the below guidelines for customer acceptance:

i. The company shall not open any account with any fictitious or anonymous or benami name or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

ii. In case where appropriate customer due diligence measures cannot be applied, account of the customer shall not be opened. This means that if the identity as submitted by the customer cannot be established or documents submitted by the customers are not as per the company's laid down criteria, the company shall not open the account of such applicant.

iii. While executing the transactions, it should be ensured that due diligence has been exercised by the company. No transactions to be executed for customers where it is not possible to

apply the due diligence measures and the company may consider closing the accounts of such customers.

iv. While applying the due diligence process, it should be ensured that it does not result into transaction becoming restrictive and should not result into denial of service.

v. Due diligence Procedure is followed for all the borrowers and Co-borrowers including guarantor, co guarantor, property owners, if any or any other person who is associated with credit facility given to borrower s, while opening a Loan account.

vi. If an existing KYC compliant customer of a company desires to open another account with the same company, there shall be no need for a fresh CDD exercise.

vii. While verifying the identity of the customer, the company shall ensure that identity as presented by the customer does not match with any person or entity whose name is appearing in the sanction lists issued by the RBI. In order to comply with this, the company shall maintain a database of negative list and use it for the purpose of screening.

viii. The list of documents to be collected from the customer shall be prepared and would be shared with the company staff and adequate training shall be provided to them. The list of documents should be revised and updated at a regular interval.

ix. For any information required from the customer for the purpose of account opening or maintenance, the company shall explicitly obtain the consent of the customer while obtaining such data.

x. In cases where accounts are operated on behalf of someone (beneficial owner) or when accounts are to be operated by mandate holder or power of attorney holder, information shall be obtained from the customer at the time of account opening.

xi. In case where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

xii. 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).

xiii. Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his customers, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk.

6.2 Customer Identification

Customer identification procedures are made to ensure that the customers are identified by using reliable, independent source documents, data or information. The company should obtain information necessary to establish to its satisfaction the true identity of each customer and the purpose of the intended nature of companying relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed

based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers.

Customer identification is required in the below scenarios:

i. At the time of commencement of an account-based relationship with the customer i.e. on boarding of the customer.

ii. While carrying out financial transactions of the customer.

iii. If there is doubt or suspicion about the authenticity of the documents submitted by the customer for the purpose of his identification.

iv. When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

v. When selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

vi. Carrying out transactions for a non-account based customer, that is a 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.

vii. When a Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the company, shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:

i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

ii. Adequate steps are taken to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

iii. 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.

iv. The third party shall not be based in a country or jurisdiction assessed as high risk.

v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, is with the Company.

In order to complete the activity of customer identification, the company shall obtain information/documents from the customer at the time of on boarding or periodic updation. The type of documents to be collected would depend on the type of customer (individual, corporate, etc.)

While deciding the acceptable documents, the below factors have to be considered:

- The document should establish the legal status of the customer.
- The document should also establish the authority of the person, acting on behalf of the customer.
- The ultimate ownership of the legal entity should be established from the documents submitted. The beneficial owners who ultimately control the legal entity should be identifiable.
- An indicative list of documents to be collected from the customers is appended in Annexure I.

6.3 Monitoring Of Transactions – Anti-Money Laundering

For KYC and AML procedures to be effective, ongoing monitoring is an essential element. The company shall understand normal and reasonable activity of the customer so as to identify the transactions that fall outside the regular pattern of activity. By doing so, the company shall effectively control and reduce the risk by having an understanding of suspicious transactions. The extent of monitoring shall depend on the risk sensitivity of the customer.

The company is a non-deposit taking NBFC. The transactions with the customer are for disbursal of loan, repayment of EMI, payment of interest, penal charges, fee or other service charges. No other transaction, other than that related to loan, shall be entered into with the customer.

Threshold limits should be prescribed for different category of borrower for the purpose of monitoring. Threshold can be fixed for:

- Transactional basis – EMI to be paid by borrower or the loan amount to be repaid
- Turnover thresholds – Total EMIs, Penal charges, interest, fee payable

Periodic checking of customer database with the watch list will be done through a system after the customer has been on-boarded, monitoring of transactions in customer accounts based on customer profile, customer type, nature of business /profession, number and value of transactions, different types of transactions, monthly turnover in the account, very large / suspicious transactions, etc. and draw various reports from historic data based on parameters defined etc.

Special attention shall be given to all complex, unusually large transactions and all patterns, which have no apparent economic or visible lawful purpose.

All transactions of suspicious nature shall be reported to Principal Officer as and when the transactions are found to be suspicious by the branches/AML Unit. The Principal Officer shall further be responsible to report such transactions to the relevant authorities.

6.4 Risk Management

It is imperative to manage the risk arising out of money laundering and non-adherence to the KYC norms. The company is exposed to various kinds of risks like reputation risk, operational risk, compliance risk and legal risk, as described below:

- Reputation risk – risk arising due to impact in reputation of the company due to non-compliances or fraud.
- Compliance risk – risk arising due to non-compliance with the regulations and guidelines
- Operational risk – risk due to failed or inadequate internal processes, people and systems.
- Legal risk – risk arising due to any legal cases being raised against the company.

In order to manage the risk arising from transactions with customers, the company shall categorize the customers into 3 risk categories –

- High risk
- Medium risk
- Low risk

The risk category shall be arrived at after considering the below factors:

- Identity of customer
- Social/financial status of customer
- Nature and industry of customer's business
- Information about the customers' business
- Location of the customer's place of business
- Any adverse news in the market about the customer
- Association or influence of Politically Exposed Person (PEP)
- Country with which import/export dealings take place

Cases where there is a higher probability of incurring risk shall be categorized as medium or high. As a result, higher due diligence measures shall be taken for such cases. The extent of due diligence requirement varies from case to case based on the assessed risk while giving the loan to the customer.

A customer profile shall be prepared containing information like customer's identity, social and financial status, background, etc. Such customer profile to be kept as confidential.

7 MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment exercise should be carried out annually to identify, assess and take effective measures to mitigate the money laundering and terrorist financing risk arising from clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The risk assessment should be commensurate to size, geographical presence, complexity of activities/structure, etc. of the Company. The risk assessment should also take cognizance of the overall sector-specific vulnerabilities, if any, that RBI may share time to time.

Risk Based Approach (RBA) should be applied for mitigation and management of risks identified and Board approved policies, controls and procedures in vogue should be accordingly aligned. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the Company, regulation and related issues will be ensured.

8 OFFICIALLY VALIDATED DOCUMENTS

As per RBI guidelines, 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, letter issued by the National Population Register containing details of name and address.

OVDs are used as a proof of identity and proof of address of customer.

A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD submitted for proof of identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

Similarly, a customer is required to submit only one OVD as proof of address (either current or permanent) for KYC purpose.

8.1 E-KYC

e-KYC authentication facility, as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction.

While establishing the relationship with the customer based on Aadhaar number, e-KYC authentication (biometric or OTP based) or Yes/No authentication shall be carried out.

'Yes/No authentication facility', as defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number

securely submitted with the consent of the Aadhaar number holder through a requesting entity. It is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing 'Yes' or 'No', along with other technical details related to the authentication transaction, but no identity information.

The conditions for carrying out the e-KYC authentication or Yes/No authentication are:

i. For account-based relationships, yes/no authentication is not allowed.

ii. If yes/no authentication is allowed, biometric or OTP based e-KYC authentication will be carried out within a period of six months

iii. Yes/No authentication in respect of beneficial owners of a legal entity shall suffice in respect of existing accounts or while establishing an account based relationship.

iv. Biometric based e-KYC authentication can be done by company official/business correspondents/business facilitators/ Biometric enabled ATMs.

The accounts opened using e-KYC shall be subject to below conditions:

i. Customer consent to be obtained for OTP based authentication

ii. Term loans shall be only be sanctioned for such customer.

iii. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

iv. Within 1 year, Biometric based e-KYC authentication shall be completed. If not, no further debits shall be allowed after 1 year.

v. Only 1 account to be opened based on OTP based KYC. Customer declaration to be obtained to such effect (to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face to face mode)

vi. Mechanism shall be put in place to generate alerts for identifying non-compliance to above conditions.

9 CUSTOMER DUE DILIGENCE (CDD)

For undertaking CDD, either of the following should be obtained from an individual or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

Sr. No.	Nature of the Document	Type of Verification
I	Proof of possession of Aadhaar number where offline verification can be carried out	Offline verification
II	Proof of possession of Aadhaar number where offline verification cannot be carried out	Digital KYC as specified under Annex - I
III	Any OVD containing the details of identity and address	Digital KYC as specified under Annex – I
IV	Any equivalent e-document of any OVD containing the details of identity and address	Verification of Digital signature and Live photo as specified under Annex - I

Note : For a period not beyond such date as may be notified by the Government for the NBFCs, instead of carrying out Digital KYC, certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph (where an equivalent e-document is not submitted) may be obtained.

a. Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962

b. The live V-CIP may be carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining informed consent with adherence to stipulations as per Annex - II

c. Offline verification of a customer may be carried out, if the customer desires to undergo Aadhaar offline verification for identification purpose. Offline Verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

In case the CDD is outsourced, then the records or the information of the customer due diligence carried out by the third party should be obtained within two days from the third party or from the Central KYC Records Registry. In such cases, decision-making functions of determining compliance with KYC norms should not be outsourced.

CDD procedure should be applied at the UCIC level and if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise.

In case of Video based Customer Identification Process (V-CIP):

V-CIP may be carried out for

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. In case of CDD of a proprietorship firm, equivalent e-document of the activity proofs with respect to the proprietorship firm should be obtained, as mentioned in Sec. 7.2 of this Policy apart from undertaking CDD of the proprietor.

ii) Updation/Periodic updation of KYC for eligible customers

9.1. ONGOING DUE DILIGENCE

An ongoing monitoring mechanism shall be established by the company to ensure that the customer's transaction are in line with their profile.

As per the RBI guidelines, close monitoring shall be mandatorily done for following type of transactions:

- Complex and large transactions which do not make any economic sense and are not consistent with the regular transactions done by the customer.
- Transactions above the threshold specified.
- High account turnover, not consistent with the amount of loan

While conducting the ongoing due diligence, regard should be given to the risk category of the customer. Customers classified as high-risk category shall be subject to more intensive monitoring than the low risk accounts.

The company shall also put in place a system for review of risk category of the customer accounts. The frequency of such review will be at least once in six months.

10 ENHANCED DUE DILIGENCE

In the below scenarios, enhanced due diligence process shall be applied for the customers:

1) Politically Exposed Persons (PEP) – While establishing a relationship with PEP or in cases where the PEP is beneficial owner, the company shall ensure the following conditions:

   - Obtain sufficient information about sources of funds
   - Verify the identity of the customer
   - Senior level approval to be taken for onboarding of PEP exposed customer (even for cases when existing beneficial owner or customer subsequently becoming a PEP)
   - Such accounts to be subject to enhanced monitoring on ongoing basis

2) The company would also adopt enhanced measures for products, services and customers with medium to high rating.

11 PERIODIC UPDATIONS OF KYC RECORDS

Based on the risk category of the customer, the company shall carry out the updation of records:

Risk Category of customer	Periodicity of review
High	Once in 2 years
Medium	Once in 8 years
Low	Once in 10 years

These time limits (2/8/10 years) are counted from the date of account opening or date of last KYC review, whichever is later.

The following activity shall be performed in the periodic updation:

a. Individual Customers:

i. **No change in KYC information**: In case of no change in the KYC information, a self-declaration from the customer in this regard to be obtained through customer's email-ID, customer's mobile number registered with us, Mobile application, Letter etc.

ii. **Change in address**: A copy of OVD or deemed OVD or equivalent e-documents as per KYC Policy for the new address to be obtained from the customer through customer's email-ID, customer's mobile number registered with us, Mobile application and Letter etc.

b. Customers other than individuals:

i. No change in KYC information: In case of no change in the KYC information of the LE customer, a self-declaration to be obtained from the LE customer through its email ID registered, mobile application, letter from an official authorized by the LE in this regard, board resolution etc. Beneficial Ownership (BO) information available to be reviewed and updated.

ii. Change in KYC information: To undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

c. Additional measures:

i. If the validity of the CDD documents available with us has expired at the time of periodic updation of KYC, KYC process equivalent to that applicable for on-boarding a new customer to be undertaken.

ii. Customer's PAN details, if available, to be verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. An acknowledgment is to be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation.

iv. The information / documents obtained from the customers at the time of periodic updation of KYC are to be promptly updated in our records / database and an intimation, mentioning the date of updation of KYC details, is to be provided to the customer.

v. Facility of periodic updation of KYC to be made available at any branch,

During periodic updation, customers' KYC details are to be migrated to current Customer Due Diligence (CDD) standards as per updated KYC Policy

If an existing KYC compliant customer desires to open another account with the organization, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

11.1 Updation of E-Kyc Accounts

For accounts opened based on e-KYC, the biometric based e-KYC authentication should be completed within 1 year. If it is not completed, a debit freeze to be marked on the account and no further debits to be allowed.

12 RECORD MANAGEMENT

The company shall make appropriate arrangements for maintenance and preservation of records and account information in a manner that enables quick retrieval, as and when required. The records should be presented to the competent authorities, as and when requested for.

S.No.	Records pertaining to	Timelines to maintain record	Type of record
1.	All records of transaction between the company and customer	For at least 5 years from the date of transaction	Soft copy/hard copy
2.	Records of customer identification and customer address, obtained at the time of account opening or during the course of relationship	For at least 5 years from the date of closure of the business relationship	Soft copy/hard copy

The company shall also maintain records of transactions as prescribed in the Rule 3 of the PML Rules 2005. These records should be maintained to an extent that allows reconstructing the transaction, including the records of :

- 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

13 RECORD MANAGEMENT REPORTING TO FIU IND

The Principal Officer will report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110 021

The format of submitting the CTR/STR in editable electronic utilities is available on the website of FIU-IND (http://fiuindia.gov.in)

The company should ensure that:

1) The account for which STR has been filed is not restricted for entering into any transaction

2) Customer is not tipped off with any details of reporting being done to the authority.

3) In case, the customer does not complete the transaction on being asked any additional information, such transaction should be reported under STR.

4) While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation.

Below are the reporting requirements as per the guidelines:

Name of the report	Transactions to be reported	Timelines of reporting
Cash Transaction Reports (CTR)	• All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency. • All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month (Integrally connected cash transactions would mean all the cash transactions in a month where the sum of either the debits or the credits in the account exceeds Rs. 10 lakhs in a month) (The conversion of foreign currency into INR shall be done at the RBI reference rate) **Note - However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated.** **CTR should contain only the transactions carried out by the NBFC on behalf of their customers/customers excluding transactions between the internal accounts of the NBFC**	To be filed for each month to FIU-IND by 15th of the succeeding month. Responsibility – Principal Officer Note – The reporting of such transactions by the branch/office of NBFC to Principal Officer to be done on monthly basis. The Principal Officer shall then submit the report to FIU IND as per above mentioned timelines.
Counterfeit Currency Report (CCR)	**All cash transactions where forged or counterfeit currency notes or notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions**	**To be filed for each month to FIU-IND by 15th of the succeeding month.** **Responsibility – Principal Officer**
Suspicious Transaction Report (STR)	To be filed for all suspicious transactions. Suspicious transaction includes an attempted transaction, whether or not made in cash which, to a person acting in good faith:	To be filed for each transaction to FIU-IND not later than seven working days on being satisfied that the transaction is suspicious.

	• 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 have no economic rationale or bonafide purpose; or • gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism; Note - The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. In order to identify suspicious transactions, the company shall have in place a robust software that can throw alerts if the transactions are inconsistent with the customer's profile.	Responsibility – Principal Officer

14 COMBATING FINANCING OF TERRORISM

The company shall take adequate steps to identify the customers that have or are suspected to have a link with sanction list which is periodically approved by the United Nations Security Council (UNSC).

Negative list screening - As and when list of individuals and entities approved by Security Council Committee, established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is received from Government of India, Reserve Bank circulates these to all companies and financial institutions. The company shall have a screening mechanism in place to identify any linkage to the entities appearing in the lists below:

i) "Al-Qaida Sanctions List", which is maintained by the 1267 / 1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

ii) "1988 Sanctions List", which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/committees/1988/list.shtml

iii) Consolidated list for Individuals and Entities is also available under the link http://www.un.org/sc/committees/consolidated_list.shtml 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 as required under UAPA notification dated August 27, 2009.

14.1 Transactions with jurisdictions that do not or insufficiently apply the FATF recommendations

Certain countries do not or insufficiently apply the FATF recommendations. A list of such countries is updated and published from time to time.

As and when RBI updates such list, the company shall ensure to consider risk arising out of such jurisdictions. The company shall give special attention to transactions with persons from such jurisdictions.

The company has identified such countries (as per current available list of countries) as high-risk countries and customers from such countries shall be classified as high risk customers. The company shall keep on updating the list as and when notifications are received from the RBI. The company shall also consider the publicly available information for identifying such countries. Countries identified by Financial Action Task Force (FATF) as "High Risk and other monitored Jurisdictions" (http://www.fatf-gafi.org/countries/#high-risk)

Further, the company shall examine the background and purpose of transactions with persons from such countries. If the transactions have no apparent economic or visible lawful purpose, the

background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank /other relevant authorities, on request.

15 ISSUANCE OF UCIC

A Unique Customer Identification Code (UCIC) shall be allotted to each customer of the company for identification of customers, to avoid multiple identities, to track the facilities availed, to monitor financial transactions and ensure better approach for risk profiling the customers.

16 SECRECY OBLIGATIONS AND SHARING OF INFORMATION

While adhering to the norms of KYC and during the course of transactions, the company obtains a lot of customer confidential information. In order to avoid misuse of the same, the company shall take all steps to maintain the confidentiality of data and avoid any loss of data. The company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the company and customer. The company has a Privacy policy which should be referred to for further details.

In several instances, the company gets requests from Government and other agencies to share the customer data/information. While considering fulfilling such requests, the company shall ensure that the information asked for does not violate the provisions of the laws relating to secrecy in the companying transactions.

In certain scenarios listed below, data/information can be shared with the requesting authority:

- Where disclosure is under compulsion of law,

- Where there is a duty to the public to disclose,
- The interest of company requires disclosure and
- Where the disclosure is made with the express or implied consent of the customer.

17 EMPLOYEE TRAINING AND HIRING OF EMPLOYEES/ACCOUNTABILITY

In order to adequately implement the KYC and AML norms, it is imperative to impart the knowledge to staff about such norms. The company staff dealing with customers are the representatives of the company and thus it is very essential to make them understand the guidelines and repercussions of the breaches thereof.

i) The company shall put in place an ongoing employee training program to ensure that the staff is adequately trained in KYC procedures. Training requirements shall be tailored made as per the need of the staff and the level of work handled by them. The training should have different focuses for frontline staff, compliance staff and staff dealing with new customers.

ii) Further, the company shall also put in place an adequate screening mechanism as a part of the employee recruitment procedure to ascertain the background of the employees.

iii) Further as one of the Human Resource functions, verifying identity of the potential employees (payroll / outsourced) and screening their names against negative / criminal lists would be carried out such that the risk of criminal, entering as employee can be minimized to a large extent by the company. Employees would be expected to adhere to the stipulated procedures / responsibilities efficiently. Any indifferent or suspicious behaviour of an employee(s) shall be dealt suitably by the company.

18 ACCOUNTS OF POLITICALLY EXPOSED PERSONS (PEPS) RESIDENT OUTSIDE INDIA

Politically exposed persons are individuals, who are or have been entrusted with prominent public functions in a foreign country e.g. heads of states or of governments, senior politicians, senior government / judicial / military officers, senior executives of state owned corporations, important political party officials etc. Decision to deal with such persons as a customer shall be taken up at a senior management level (SVP and above) and should be subjected to enhanced monitoring. The norms are also applied to the accounts of the family members or close relatives of PEPs. In case of an existing customer or beneficial owner of an existing account subsequently becoming PEP, matter should be reported to senior management level and be subjected to enhanced monitoring.

19 ACCOUNTS OF NON-FACE-TO-FACE CUSTOMERS

In the case of non-face-to-face customers, it should be ensured that the first payment is effected through the customer's KYC-complied account with another regulated entity.

20 CENTRAL KYC REGISTRY (CKYCR)

The customer KYC information should be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities

(LE)' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

The customer information related to LEs should be submitted to CKYCR for accounts of LEs opened on or after Apr 1, 2021.

For accounts of LEs opened prior to Apr 1, 2021 and account of Individuals opened prior to Jan 01, 2017, KYC records are to be uploaded to CKYCR during the periodic updation, (carried out once in every two years for high risk customers, eight years for medium risk and ten years for low risk) or earlier as and when KYC information is obtained/received from customer.

Further, during periodic updation, customers' KYC details are to be migrated to current Customer Due Diligence (CDD) standards.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and customer is not required to submit any KYC records unless

a. there is a change in information of customer as existing in the records of CKYCR;

b. current address of customer is required to be verified;

c. it is considered necessary to verify identity or address of customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

KYC Identifier generated by CKYCR, should be communicated to the Individual/LE.

21 INDICATIVE LIST OF DOCUMENTS TO BE COLLECTED FROM THE CUSTOMERS

Identification as under, would be required to be obtained in respect of different classes of customers:

a. Customers that are natural persons:

i. Address/location details
ii. Identity Proof and Recent photograph

b. Customers that are legal persons:

i. Legal status of the legal person/entity through proper and relevant documents.
ii. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person is established and verified.
iii. Understand the ownership and control structure of the customer and determine who are the natural persons and ultimately control the legal person.

Individual Customers (Mandatory Pan Number)

a. The customers would submit OVD for identity and address.
b. Individual customers have to mandatorily submit the Permanent Account Number or Form No. 60. This would also apply to individuals who are beneficial owner, authorized signatory or power of attorney holder related to any legal entity.

For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

Proprietorship Firms:

Documents which could be obtained as proof of business/activity for proprietary firms (any one), in addition to the documents of the proprietor as individual:

a. Registration Certificate
b. Certificate/ license issued by the Municipal authorities under Shop & Establishment Act,
c. Sales and Income tax returns,
d. CST / VAT/GST certificate (Provisional/Final)
e. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of Director General of Foreign Trade (DGFT)/License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statue
g. Complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected duly authenticated / acknowledged by the Income Tax Authorities
h. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern

Any one of the above documents in the name of the proprietary concern would suffice.

Partnership Firms:

Where the customer is a partnership firm, the certified copies of the following documents should be obtained:

a. PAN of the partnership firm
b. Certificate of registration
c. Partnership deed.
d. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
e. Permanent Account Number or Form 60 of the persons holding an attorney to transact on its behalf along with any OVD for identity and address proof and one recent photograph of such persons.

Trusts:

Where the customer is a trust firm, the certified copies of the following documents should be obtained:

a. PAN/Form No. 60 of the entity
b. Certificate of registration
c. Trust deed.

d. Power of Attorney granted to a member or an employee of the firm to transact business on its behalf
e. Permanent Account Number or Form 60 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.

Unincorporated Bodies:

Where the customer is an unincorporated association or a body of individuals, the certified copies of the following documents should be obtained:

a. PAN/Form No. 60 of the entity
b. resolution of the managing body of such association or body of individuals;
c. power of attorney granted to him to transact on its behalf
d. Permanent Account Number or Form 60 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.

Companies:

Where the customer is a Company, the certified copies of the following documents should be obtained:

a. PAN of the Company
b. Certificate of incorporation
c. Memorandum and Articles of Association
d. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with their Permanent Account Number or Form 60 and any OVD or Aadhaar card for identity and address proof and one recent photograph of such persons.

For opening accounts of juridical persons not specifically covered above, such as Government or its Departments, societies, universities and local bodies like village panchayats, one certified copy of the following documents should be obtained:

i. Document showing name of the person authorized to act on behalf of the entity;
ii. Officially valid document for proof of identity and address in respect of the person holding an attorney to transact on its behalf and one recent photograph and
iii. Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

a. General guidelines for collecting the documents

The below mentioned points should be adhered to by the RMs/the processing team at the time of collection and verification of the documents:

- Duly completed application forms signed by the applicants/Guarantor
- Cross sign on all Individual applicants/guarantors photograph

- Latest passport size coloured photograph of all applicants and guarantors
- Any corrections/overwriting on the application form should be countersigned by the respective applicants
- In some of cases, wherein the relationship between applicant and co-applicant & guarantor is not clearly established & they are blood relatives. COMPANY'S may take a declaration on COMPANY'S approved format from the applicant regarding the same. Declaration should be stamped as per the applicable stamp law
- All documents provided by the customer should be sighted in original and verified by the sales executive, DSA or Digital Channel. OSV (Original seen & verified) stamp to be affixed along with name, signature & employee id (if Company's employee) of the verifier. Bio-metric check can also be considered in lieu of OSV
- All documents should be self-attested by the respective applicants/guarantor
- Requirement of fresh KYC and income documents from an existing customer would be at sole discretion of Company's
- Aadhaar card / E-Aadhaar to be taken as a mandatory KYC document
- GSTIN Registration certificate to be taken as a mandatory KYC document
- Ration card not to be accepted as address proof
- Expired KYC document at the time of Disbursement will not be considered as valid KYC document
- If company/firm registered & current address is different than valid address proof of both addresses would be required
- If property is on rent then we can't consider the property papers as valid address proof
- If customer is depositing BSV / Gazetted officer letter / Banker letter then original letter would be considered as valid KYC document.

Dual Name Affidavit:

There are cases, where there are mismatches in the names on the application form and the identity proof due to –

- Mistake occurred/committed by the issuing authority of the ID proof
- Change of surname after marriage
- Same individual having different name mentioned in application form and KYC documents submitted (usage of title)
- Elaboration of initials detailing applicant's first/ middle name & surname.

In such scenario, the declaration for dual name should be obtained on stamp paper with applicable stamp duty. The declaration should be in company's format only.

Dual Signature Affidavit:

In case, where customer has two different signatures on two different documents (as per the list given above under signature proof doc) then in such cases, one of the signatures should match with the signature on application form & other loan documents. A dual sign affidavit should be obtained on stamp paper with applicable stamp duty. The declaration should be in company's format only.

No signature proof affidavit:

This Affidavit can be taken in case any co-applicant / Guarantor does not have any kind of Signature proof provided-

- He / She is not primary Applicant
- His / Her income is not considered while giving loan facility

The declaration should be in company's format only.

Dual Date of Birth Affidavit:

In case where customer has two different date of birth on two different documents, (as per the list given above under DOB proof doc) then in such cases, one of the DOB should match with mentioned DOB on application form & the same DOB should be captured on system. A dual DOB affidavit should be obtained on stamp paper with the applicable stamp duty. The declaration should be in company's format only.

 # Stamp paper for all above mentioned affidavits should be purchased in the name of declaring person only & affidavit should be notarized. Stamp duty will be applicable as per state law.

* Notwithstanding the list of documents as stated above, in case of change, if any, in the regulations as notifies by RBI from time to time, the list of documents as prescribed by RBI shall prevail over the above.

** In case of proprietary concern, the documents shall be in the name of the concern

Note:

1. All the applicants shall have valid ID proof as prescribed above.

2. 'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the documents mentioned below for the purpose of –

A. Proof of identity -

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

B. Proof of address -

The following documents shall be deemed to be officially valid documents for low risk' customers for the limited purpose of proof of address where customers are unable to produce —any-officially valid document for-the-same:-

- Bank account or Post Office savings bank account statement
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
- Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
- Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

22 REVIEW OF POLICY

The Board of Directors reserves its right to review and amend this policy to ascertain its appropriateness as per the needs of the company. Review shall be carried out at least once a year. In the event of any conflict between the provisions of this Policy and the RBI/ SEBI Regulations or any other statutory enactments, rules, the provisions of such RBI/ SEBI Regulations or statutory enactments, rules shall prevail over this Policy.

The Board may, subject to applicable laws amend any provision(s) or substitute any of the provision(s) with the new provision(s) or replace the Policy entirely with a new Policy.

ANNEX - I DIGITAL KYC PROCESS

A. A Digital KYC Application (KYC App) for digital KYC process is to be made available at customer touch points and is to be undertaken only through this authenticated application of the Company

B. Access of the KYC App to be controlled and be ensured that it is not used by any unauthorized person.

C. KYC App to be accessed only through Login-ID and Password, Live OTP or Time OTP controlled mechanism given to the authorized officials of the Company

D. Customer, for KYC, should visit the location of the authorized official of the Company or vice versa. The original OVD should be in possession of the customer.

E. Live photograph of the customer should be taken by the authorized officer and the same photograph should be embedded in Customer Application Form (CAF).

F. KYC App should add a water-mark in readable form having 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.

G. KYC App should have a feature such that only live photograph of the customer is captured and not printed or video-graphed photograph.

H. Background behind the customer should be white and no other person should come into frame

I. Live photograph of original OVD or proof of possession of Aadhaar (if offline verification is not being done) placed horizontally, should be captured vertically from above and water-marking as stated above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

J. Live photograph of customer and original documents should be captured in proper light so that they are clearly readable and identifiable.

K. All the entries in the CAF should be made as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details.

L. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' is to be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF.

M. In case, the customer does not have his/her own mobile number, mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF.

N. In any case, the mobile number of authorized officer registered with the Company should not be used for customer signature.

O. It must be verified that mobile number used in customer signature is not mobile number of authorized officer.

P. Authorized officer should provide a declaration about capturing live photograph of customer and original document. For this purpose, authorized official should be verified with OTP sent to the mobile number registered with the Company. This OTP validation is to be treated as authorized officer's signature on the declaration. Live photograph of authorized official should also be captured in the authorized officer's declaration.

Q. Subsequent to all these activities, the KYC App should give information about the completion of the process and submission of activation request to an activation officer of the Company, and also generate transaction-ID/reference-ID number of the process. Authorized officer should intimate the details regarding transaction-ID/reference-ID number to customer for future reference.

R. Authorized officer of the Company should verify that

i. information available in picture of document is matching with information entered in CAF

ii. live photograph of the customer matches with the photo available in the document

iii. all the necessary details in CAF including mandatory fields are filled properly

S. On Successful verification, the CAF should be digitally signed by authorized officer of the Company and the a print of CAF, should be bear signatures/thumb-impression of customer at appropriate place

T. The signed document should be scanned and uploaded in system and the original hard copy should be returned to the customer.

ANNEX – II VIDEO CUSTOMER IDENTIFICATION PROCESS (V-CIP)

A. Live V-CIP should be carried out by an official of the Company after obtaining customer's informed consent

B. Video of the customer should be recorded along with photograph

C. For identification of the customer, offline verification of Aadhaar should be conducted

D. Clear image of PAN card displayed by customer should be captured, except in cases where e-PAN is provided. PAN details should be verified from Income Tax department.

E. Live location of customer (Geotagging) should be captured to ensure that customer is physically present in India

F. Photograph in Aadhaar/PAN details should match with the customer and the identification details in Aadhaar/PAN should match with details provided by customer.

G. Sequence and/or type of questions during video interactions should be varied in order to establish that interactions are real-time and not pre-recorded.

H. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the XML file or QR code generation date should not be older than 3 days from the date of carrying out V-CIP.

I. Accounts opened through V-CIP should be operational only after being subjected to concurrent audit

J. Process should be 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.

K. Liveliness check should be carried out in order to guard against spoofing and such other fraudulent manipulations.

L. To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application should be carried out before rolling it out.

M. Interaction should be triggered from the domain of the Company, and not from third party service provider

N. Process should be operated by officials specifically trained for this purpose and activity log along with the credentials of the official performing the V-CIP should be preserved.

O. Video recording should be stored in a safe and secure manner and bear the date and time stamp

P. Assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies may be taken, to ensure the integrity of the process as well as the information furnished by the customer.

(a) V-CIP Infrastructure

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

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

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

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

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the RE. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

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

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

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

(b) V-CIP Procedure:

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

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

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

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

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

(vi) The authorized official of the Organization performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) KYC records downloaded from CKYCR, in accordance with Master direction, using the KYC identifier provided by the customer

b) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker Organization shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of Master Direction.

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 days from the date of carrying out V-CIP.

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

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

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

(c) V-CIP Records and Data Management:

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

(ii) The activity log along with the credentials of the Organization official performing the V-CIP shall be preserved.

Annex – III : Illustrative list of suspicious transactions

(i) <u>Illustrative list of suspicious transactions pertaining to builder Project / corporate clients</u>:

1) Builder approaching company for a small loan compared to the total cost of the project;

2) Builder is unable to explain the sources of funding for the project;

3) Approvals/sanctions from various authorities are proved to be fake or if it appears that client does not wish to obtain necessary governmental approvals/ filings, etc.;

4) Management appears to be acting according to instructions of unknown or inappropriate person(s).

5) Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).

6) Clients with multijurisdictional operations that do not have adequate centralized corporate oversight.

7) Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/ corporate seat or other complex group structures).

8) Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.

(ii) Illustrative list of suspicious transactions pertaining to individuals :

1) Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).

2) Unnecessarily complex client structure.

3) Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear.

4) Customer is reluctant to provide information, data, documents;

5) Submission of false documents, data, purpose of loan, details of accounts;

6) Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;

7) Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;

8) Approaches a branch/ office of a company, which is away from the customer's residential or business address provided in the loan application, when there is company branch / office nearer to the given address;

9) Unable to explain or satisfy the numerous transfers in account/ multiple accounts;

10) Initial contribution made through unrelated third party accounts without proper justification;

11) Availing a top-up loan and/ or equity loan, without proper justification of the end use of the loan amount;

12) Suggesting dubious means for the sanction of loan;

13) Where transactions do not make economic sense;

14) Unusual financial transactions with unknown source.

15) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

16) There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;

17) Encashment of loan amount by opening a fictitious bank account;

18) Applying for a loan knowing fully well that the property/dwelling unit to be financed has been funded earlier and that the same is outstanding;

19) Sale consideration stated in the agreement for sale is abnormally higher / lower than what is prevailing in the area of purchase;

20) Multiple funding of the same property/dwelling unit;

21) Request for payment made in favour of a third party who has no relation to the transaction;

22) Usage of loan amount by the customer in connivance with the vendor/builder/developer/broker/agent etc. and using the same for a purpose other than what has been stipulated.

23) Multiple funding / financing involving NCO / Charitable Organization / Small/ Medium Establishments (SMEs) / Self Help Croups (SHCs) / Micro Finance Croups (MFCs);

24) Frequent requests for change of address;

25) Overpayment of installments with a request to refund the overpaid amount;

26) Investment in real estate at a higher/lower price than expected;

27) Clients incorporated in countries that permit bearer shares.